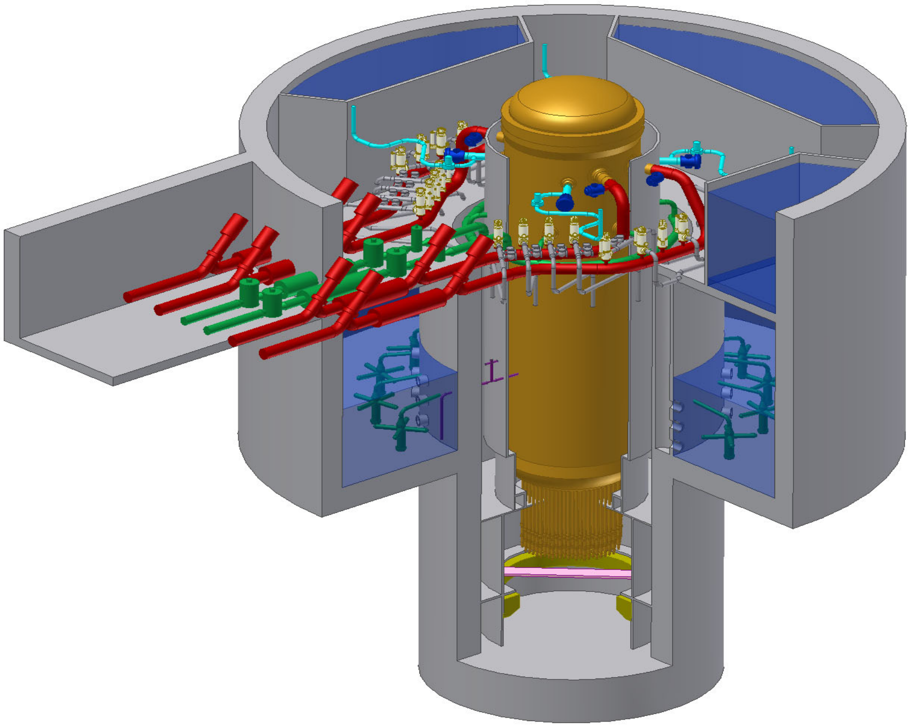
GE Nuclear Energy

26A6642BZ
Revision 0
August 2005



ESBWR Design Control Document

Tier 2

Chapter 19

PRA & Severe Accident

(Conditional Release – pending closure of Design Verifications.)

Contents

List of Tables

List of Illustrations

Global Abbreviations And Acronyms List

10 CFR	Title 10, Code of Federal Regulations
ac	Alternating Current
ACF	Automatic Control Function
ACS	Atmospheric Control System
ADS	Automatic Depressurization System
ALWR	Advanced Light Water Reactor
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transients Without Scram
BiMAC	Basemat Internal Melt Arrest and Coolability System
BMP	Basemat Melt Penetration
BWR	Boiling Water Reactor
CBP	Containment Bypass and Leakage
CCFP	Conditional Containment Failure Probability
CCI	Corium-Concrete Interactions
CDF	Core Damage Frequency
CET	Containment Event Tree
CFR	Code of Federal Regulations
CIV	Combined Intermediate Valve
CLCH	Convection-Limited Containment Heating
COL	Combined Operating License
COP	Containment Over-Pressurization
COPS	Containment Over-pressure Protection System
CPET	Containment Phenomenological Event Tree
CRD	Control Rod Drive
CRDHS	Control Rod Drive Hydraulic System
CRSS	Center for Risk Studies and Safety
CSET	Containment System Event Tree
CST	Condensate Storage Tank
CV	Containment Vessel
dc	Direct Current
DCH	Direct Containment Heating

DCS	Drywell Cooling System
DG	Diesel-Generator
dPT	Differential Pressure Transmitter
DPV	Depressurization Valve
DW	Drywell
EPRI	Electric Power Research Institute
EVE	Ex-Vessel Steam Explosion
FAPCS	Fuel and Auxiliary Pools Cooling System
FCI	Fuel-Coolant Interactions
GDC	General Design Criteria
GDCS	Gravity-Driven Cooling System
GE	General Electric Company
GE-NE	GE Nuclear Energy
HFE	Human Factors Engineering
HP	High Pressure
HPME	High Pressure Melt Ejection
HPNSS	High Pressure Nitrogen Supply System
HVAC	Heating, Ventilation and Air Conditioning
HX	Heat Exchanger
I&C	Instrumentation and Control
I/O	Input/Output
IAS	Instrument Air System
IC	Isolation Condenser
ICD	Interface Control Diagram
ICS	Isolation Condenser System
IEEE	Institute of Electrical and Electronics Engineers
IIS	Iron Injection System
IVR	In-Vessel Retention
LAPP	Loss of Alternate Preferred Power
LOCA	Loss-of-Coolant-Accident
LOPP	Loss of Preferred Power
LP	Low Pressure

MAAP	Modular Accident Analysis Program
MCCI	Molten Corium-Concrete Interactions
MOV	Motor-Operated Valve
MSIV	Main Steam Isolation Valve
MSL	Main Steamline
NBS	Nuclear Boiler System
NRC	Nuclear Regulatory Commission
NSSS	Nuclear Steam Supply System
PCCS	Passive Containment Cooling System
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PWR	Pressurized Water Reactor
RAM	Reliability, Availability and Maintainability
RBCC	Rod Brake Controller Cabinet
RCCV	Reinforced Concrete Containment Vessel
RCCWS	Reactor Component Cooling Water System
RCPB	Reactor Coolant Pressure Boundary
RG	Regulatory Guide
ROAAM	Risk-Oriented Accident Analysis Methodology
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown System
RTNSS	Regulatory Treatment of Non-Safety Systems
S/P	Suppression Pool
SA	Severe Accidents
SAM	Severe Accident Management
SAMS	Severe Accident Management Strategy
SAS	Service Air System
SAT	Severe Accident Treatment
SBWR	Simplified Boiling Water Reactor
SDC	Shutdown Cooling
SLCS	Standby Liquid Control System

SRP	Standard Review Plan
SRV	Safety Relief Valve
SRVDL	Safety Relief Valve Discharge Line
SSC	Structures, Systems, and Components
SSE	Safe Shutdown Earthquake
TDH	Torispherical Drywell Head
TMI	Three Mile Island
TRAC	Transient Reactor Analysis Code
UCSB	University of California, Santa Barbara
UHS	Ultimate Heat Sink
URD	Utility Requirement Documents
VAC	Volts Alternating Current
VDC	Volts Direct Current

19. PRA & SEVERE ACCIDENT

19.1 INTRODUCTION AND SUMMARY

The detailed documentation of the ESBWR Probabilistic Risk Assessment (PRA) is provided in NEDO-33201. Chapter 19 of the ESBWR DCD summarizes those aspects of the ESBWR design that are required to meet the quantified risk performance documented in the PRA.

This section provides an introduction to the regulatory requirements and safety goals associated with the ESBWR PRA and summarizes how the results of the PRA compare against these safety goals.

19.1.1 Regulatory Requirements for PRA and Severe Accidents

The Commission expects that new designs, like the ESBWR, will achieve a higher standard of severe accident safety performance than previous designs. In an effort to provide this additional level of safety in the design of advanced nuclear power plants, the NRC has developed guidance and goals for which designers should strive in accommodating events that are beyond what was previously known as the design basis of the plant.

For advanced nuclear power plants, the staff concluded that vendors should address severe accidents during the design stage. This will allow the designers to take full advantage of the insights gained from such input as probabilistic safety assessments, operating experience, severe accident research, and accident analysis by designing features to reduce the likelihood that severe accidents will occur and, in the unlikely occurrence of a severe accident, to mitigate the consequences of such an accident. Incorporating insights and design features during the design phase has been demonstrated to be much more cost effective than modifying existing plants.

The Commission issued the “Policy Statement on the Use of Nuclear Probabilistic Risk Assessment Methods in Nuclear Regulatory Activities” on August 16, 1995. This statement presented the policy that the NRC will follow in the use of probabilistic risk assessment methods in nuclear regulatory matters. The Commission adopted the following policy statement regarding the expanded NRC use of PRA:

(1) The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy.

(2) PRA and associated analyses (e.g., sensitivity studies, uncertainty analyses, and importance measures) should be used in regulatory matters, where practical within the bounds of the state-of-the-art, to reduce unnecessary conservatism associated with current regulatory requirements, regulatory guides, license commitments, and staff practices.

(3) PRA evaluations in support of regulatory decisions should be as realistic as practicable and appropriate supporting data should be publicly available for review.

(4) The Commission's safety goals for nuclear power plants and subsidiary numerical objectives are to be used with appropriate consideration of uncertainties in making regulatory judgments on the need for proposing and backfitting new generic requirements on nuclear power plant licensees.

The Commission issued 10 CFR Part 52, "Early Site Permits; Standard Design Certifications; and Combined Licenses for Nuclear Power Plants," on April 18, 1989. 10 CFR 52.47(a)(v) requires that a design-specific probabilistic risk assessment (PRA) be submitted as part of an application for standard design certification. The ESBWR PRA is contained in Licensing Topical Report NEDO-33201, "ESBWR Design Certification Probabilistic Risk Assessment" (Reference 19.1-1) which was developed concurrently with this DCD.

Specifically, 10 CFR 52.47 requires an application for design certification to include the following:

- demonstrate compliance with any technically relevant portions of the TMI requirements given in 10 CFR 50.34(f)
- propose technical resolutions of those unresolved safety issues and medium- and high-priority generic safety issues which are identified in the version of NUREG-0933 current on the date 6 months prior to application and which are technically relevant to the design
- contain a design-specific PRA

On April 2, 1993, the NRC staff issued SECY-93-087, which sought Commission approval for the staff's positions pertaining to evolutionary and passive LWR design certification policy Severe Accidents issues. Preventive feature issues addressed in SECY-93-087 relating to the ESBWR include the following:

- anticipated transient without scram (ATWS)
- station blackout
- fire protection
- intersystem loss-of-coolant accident

Mitigative feature issues addressed in SECY-93-087 relating to the ESBWR include the following:

- combustible gas control
- core debris coolability
- high-pressure core melt ejection
- containment performance
- equipment survivability

This section identifies the NRC approved safety goals and compares the results of the PRA to the safety goals. The ESBWR PRA process is summarized in Section 19.2 and documented fully in NEDO-33201.

19.1.2 NRC Safety Goals

On January 12, 1990, the NRC staff issued SECY-90-016, which requested Commission approval for the staff's recommendations concerning proposed departures from current regulations for the evolutionary light water reactors (ELWR). The Commission approved some of the staff positions stated in SECY-90-016 and provided additional guidance regarding others in an SRM dated June 26, 1990. The following PRA based safety goals are approved:

- A core damage frequency goal of 10^{-4} per year of reactor operation.
- The expected mean frequency of occurrence of events that result in a large release of radioactivity shall be less than 10^{-6} per year of reactor operation considering both internal and external events. A large release is defined as one that has a potential for causing an offsite early fatality.
- The containment conditional failure probability (CCFP) shall not exceed 0.1 when weighted over credible core damage sequences

In SECY-93-087, the staff recommended that the Commission approve the following deterministic containment performance goal for the passive ALWRs:

- The containment should maintain its role as a reliable, leak-tight barrier (for example, by ensuring that containment stresses do not exceed ASME Service Level C limits for metal containments or factored load category for concrete containments) for approximately 24 hours following the onset of core damage under the more likely severe accident challenges and, following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products.

In the SRM dated July 21, 1993, the Commission approved the staff's position to use the deterministic containment performance goal (CPG) in the evaluation of the passive ALWRs as a complement to the CCFP approach.

The Commission issued the "Policy Statement on Safety Goals for the Operation of Nuclear Power Plants" on August 4, 1986. This policy statement focused on the risks to the public from nuclear power plant operations with the objective of establishing goals that broadly define an acceptable level of radiological risk that might be imposed on the public because of nuclear power plant operation. These are the risks from release of radioactive material from the reactor to the environment from normal operations as well as from accidents. The Commission established two qualitative safety goals that are supported by three quantitative objectives. The qualitative safety goals follow:

- Individual members of the public should be provided a level of protection from the consequences of nuclear power plant operation such that individuals bear no significant additional risk to life and health.
- Societal risks to life and health from nuclear power plant operation should be comparable to or less than the risks of generating electricity by viable competing technologies and should not be a significant addition to other societal risks.

In order to meet the qualitative goals, three major offsite quantitative consequence-related goals are established as follows:

(1) Individual Risk Goal

The risk to an average individual in the "vicinity" of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one tenth of one percent (0.1%) of the sum of "prompt fatality risks" resulting from other accidents to which members of the U.S. Population are generally exposed. As noted in the Safety

Goal Policy statement, "vicinity" is defined as the area within 1.61 km (1 mile) of the plant site boundary. "Prompt Fatality Risks" are defined as those risks to which the average individual residing in the vicinity of the plant is exposed to as a result of normal daily activities. Such risks are the sum of risks that result in fatalities from such activities as driving, household chores, occupational activities, etc.

(2) Societal Risk Goal

The risk to the population in the area "near" a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one tenth of one percent (0.1%) of the sum of the "cancer fatality risks" resulting from all other causes. As noted in the Safety Goal Policy Statement, "near" is defined as within 16.1 km (10 miles) of the plant.

(3) Radiation Dose Goal

The probability of exceeding a whole body dose of 0.25 sv at a distance of 805 m (one half mile) from the reactor shall be less than one in a million per reactor year.

19.1.3 Comparison against NRC Safety Goals

This section evaluates how the goals established by the NRC that relate to the prevention or mitigation of severe accidents are met by the ESBWR. Table 19.1-1 provides a comparison of each of the NRC safety goals, including the deterministic containment performance goal and indicates how the ESBWR meets each of these goals.

Table 19.1-1

ESBWR Comparison Against NRC Safety Goals

NRC SAFETY GOAL	ESBWR COMPARISON AGAINST GOAL
Core damage frequency (CDF) of $\leq 10^{-4}$ per year of reactor operation	ESBWR baseline PRA CDF is significantly less than 10^{-4} per year of reactor operation. This is true even if only safety related and RTNSS equipment are credited, or if no operator action is assumed for 72 hours (with credit for non-safety equipment)
The expected mean frequency of occurrence of events that result in a large release of radioactivity shall be $\leq 10^{-6}$ per year of reactor operation considering both internal and external events.	ESBWR baseline PRA LRF is significantly less than 10^{-6} per year of reactor operation. This is true even if only safety related and RTNSS equipment are credited, or if no operator action is assumed for 72 hours (with credit for non-safety equipment) Conservative analysis of external events resulted in an LRF that is much smaller than the internal events contribution
The containment conditional failure probability (CCFP) shall not exceed 0.1 when weighted over credible core damage sequences	The ESBWR CCFP is significantly less than 0.1 when weighted over credible core damage sequences that occur when the containment is required to be operable.
The containment should maintain its role as a reliable, leak-tight barrier (for example, by ensuring that containment stresses do not exceed ASME Service Level C limits for metal containments or factored load category for concrete containments) for approximately 24 hours following the onset of core damage under the more likely severe accident challenges and, following this period, the containment should continue to provide a barrier against the uncontrolled release of fission products	The ESBWR meets this containment performance goal with considerable margin. The more likely severe accident sequences do not result in containment failure for 72 hours or more. The low frequency severe accident sequences do not result in containment failure in less than 24 hours. Severe accidents that can cause containment failure in less than 24 hours have a frequency low enough to be considered remote and speculative.

Table 19.1-1

ESBWR Comparison Against NRC Safety Goals

The risk to an average individual in the "vicinity" of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one tenth of one percent (0.1%) of the sum of "prompt fatality risks" resulting from other accidents to which members of the U.S. Population are generally exposed		The sum of prompt fatality risks is taken as the U.S. accidental death risk value of 39.1 deaths per 100,000 people per year ($3.91x10^{-4}$) and the risk from the ESBWR to an average individual in the vicinity of the plant is less than 0.1% of this risk.
The risk to the population in the area "near" a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one tenth of one percent (0.1%) of the sum of the "cancer fatality risks" resulting from all other causes. As noted in the Safety Goal Policy Statement, "near" is defined as within 16.1 km (10 miles) of the plant.		The "cancer fatality risk" is taken as 169 deaths per 100,000 people per year ($1.7x10^{-3}$) and the cancer risk from operation of the plant in the area near the plant is less than 0.1% of this risk.
The probability of exceeding a whole body dose of 0.25 sv at a distance of 805 m (one half mile) from the reactor shall be less than one in a million (10^{-6}) per reactor year.		The probability of a release that would exceed a dose of 0.25 sv at a distance of 0.5 miles from the plant is significantly less than 10^{-6} per reactor year.

19.2 PRA SUMMARY AND RESULTS

This section summarizes the methodology and models of the ESBWR Probabilistic Risk Assessment (PRA). The PRA has been performed in conjunction with the development of the plant design in order to provide design improvement feedback that would enhance plant safety.

The main objectives of the ESBWR PRA are:

a. To provide an integrated and systematic view of the ESBWR design in response to transient and accidents, including severe accidents,

b. To assess the adequacy of the ESBWR design with respect to human interaction,

c. To identify design and analysis areas where major investigation and/or improvement is needed to meet the safety goals,

d. To provide a tool to investigate alternative design solutions and operational strategies to optimize ESBWR plant safety,

e. To provide justification of the classification of the non-safety systems.

This section provides an overview of the ESBWR PRA and a summary of the PRA results. The overview includes the internal and external events analyses, the shutdown PRA, the severe accident progression analysis and the offsite consequence analysis. The ESBWR PRA is a full scope (Level 1, Level 2, and Level 3) PRA, that covers both internal and external events, full power and shutdown. Where applicable, ASME-RA-S-2002 capability category 3 attributes are included in the analysis. Obviously, some of these attributes are not achievable at the certification stage of a nuclear power plant. For example, many aspects of assessing human actions cannot be analyzed in absence of a physical, operating plant and operation staff. In these cases, a bounding approach is taken to encompass all potential sites, configurations, and operating organizations. In addition, any analysis requiring site specific characteristics are treated in a bounding manner.

19.2.1 Internal Events Analysis

19.2.1.1 Identification of Internal Initiating Events

Internal initiating events are those events that occur either as a direct result of equipment failure, or as the result of errors while performing maintenance, testing, or any other operator action. These events occur during normal high power operation. Initiating events are based on NURGE/CR-5750 (Reference 19.2-1). These frequencies are considered bounding for the ESBWR. No attempt is made in this report to reduce the generic frequencies by taking into account ESBWR specific scram reduction features.

Individual initiating events are grouped into categories that have the same plant response. The initiating events categories are identified below.

(1) Transients

- Generic Transient (Turbine trip or spurious reactor trip)
- Transient with power conversion system (PCS) unavailable
- Loss of feedwater transient

- Loss of the plant service water (PSW) system (including the loss of the RCCW system)
- Inadvertent opening of a SRV (IORV)
- Loss of Preferred Power

(2) LOCA

The Loss of Coolant Accidents (LOCAs) are divided into different classes based on the size and elevation of the break. In particular, the breaks in the reactor coolant pressure boundary have been classified with respect to location as follows:

- Liquid breaks for pipes connected to the RPV at an elevation lower than Level 3
- Steam breaks for pipes connected to the RPV at an elevation above Level 3, even though a liquid phase may initially be discharged through the rupture
- Breaks in pipes connected to the vessel below the top of fuel.

The size of the breaks are classified as follows:

- Large steam breaks fully depressurize the plant through the break alone
- Small steam breaks require SRVs or DPVs to fully depressurize
- There are no large liquid breaks
- Small liquid breaks can be mitigated with CRD as the only injection source
- Medium liquid breaks are those that are larger than CRD capacity

(3) Anticipated Transients Without Scram

(4) Breaks Outside Containment

19.2.1.2 Event Trees and Accident Sequences

19.2.1.2.1 Acceptance Criteria

The acceptance criteria for the critical safety functions that are required for safe plant operation are described below:

Reactivity Control

The acceptance criterion is to achieve subcriticality and maintain the reactor in a subcritical state

RPV Overpressure Protection

A pressure of 150 percent of the reactor coolant pressure boundary is defined as the acceptance criterion for the RPV overpressure protection.

Core Cooling

A peak cladding temperature (PCT) of 2200°F (calculated with a detailed core model) has been chosen as the criterion for establishing the adequacy of coolant inventory.

Containment Heat Removal

For event sequences in which core cooling is successful, the acceptance criterion for the containment cooling function is to maintain the pressure below the ultimate containment failure pressure.

19.2.1.2.2 Success Criteria

Success criteria are defined as the minimum grouping of systems that are required to operate in a timely fashion in order to meet the acceptance criteria related to the safety functions identified in the Section 19.2.1.2.1. Each specific success criterion is based on thermal-hydraulic calculations.

19.2.1.2.3 Event Tree Development

The event tree methodology is used to represent the possible sequences of events following any one of the initiating event groups defined above. Each event tree sequence depicts a possible combination of system and operator action successes or failures leading to either a successful cooling of the core or to core damage according to the acceptance and success criteria.

The event trees developed in the ESBWR PRA are:

- Generic Transient (BASE Case)
- Transient with PCS unavailable (T PCS)
- Loss of Feedwater Transient (T FDW)
- Loss of Service Water System (T SW)
- Loss of Preferred Power Transient (T-LOPP)
- Inadvertent Opening of a RV (IORV)
- ATWS from Generic Transient or LOPP (Base Case)
- ATWS from Transient Loss of PCS
- ATWS from Transient with Loss of Feedwater System
- ATWS from Transient with Loss of Service Water System
- ATWS from Inadvertent Opening of a RV
- Large steam breaks (above L3) other than Feedwater lines
- Large steam breaks (above L3) on FDW (A) lines
- Large steam breaks (above L3) on FDW (B) line
- Small steam breaks (above L3)
- Medium liquid breaks (below L3) other than RWCU/SDC lines
- Medium liquid breaks (below L3) in RWCU/SDC lines
- Small liquid LOCA (below L3) other than RWCU/SDC lines
- Small liquid LOCA (below L3) in RWCU/SDC lines

- Reactor Vessel Rupture
- Steam break outside containment on Main Steam lines
- Steam break outside containment on FDW A lines
- Steam break outside containment on FDW B lines
- Large steam break outside containment on IC lines
- Large liquid break outside containment on RWCU/SDC lines

The specific characteristics that are taken into consideration for the development of each event tree and its functions are described in the ESBWR PRA (Reference 19.1-14).

19.2.1.2.4 End States of the Accident Sequences

The end point of each of these sequences could be a stable and safe state of the plant (i.e., hot standby conditions), or a plant damage state (i.e., core melting or failure of the containment heat removal) identified as an accident class.

The end states of the accident sequences developed for the ESBWR PRA are provided below:

- OK: The core is successfully cooled for more than 72 hours
- CD I: The containment is intact when core melt occurs. The RPV is at low pressure at the time of core melt
- CD II: The containment fails while the core is successfully cooled. The core failure will occur only if the containment failure affects the core cooling
- CD III: The containment is intact when core melt occurs. The PRV is at high pressure at the time of core melt
- CD IV: Reactivity in the core is not controlled. Core melt occurs due to high core power.
- CD V: The containment is bypassed at the initiation of the accident

19.2.1.3 Systems Analysis

As part of the systems analysis, detailed fault trees are developed for all the safety systems and several non-safety systems whose operation could mitigate the effects of an accident. The fault tree analysis provides detailed modeling down to the major components in the plant. Failures on demand and during the mission of the component are both modeled. Common cause failure is treated for components used in redundant applications. The human actions that are modeled include both pre-initiator failures and post-initiator failures. Test and maintenance unavailability is also included explicitly in the systems analysis.

Table 19.1-1 summarizes the systems and functions modeled.

19.2.1.4 Data Analysis

The reliability data used in the ESBWR PRA are based on the ALWR URD (Reference 19.2-2). These data are complemented with the ABWR PRA Database (Reference 19.2-4) and other generic data sources (References 19.2-3 to 19.2-13) as necessary, following this order or preference.

The use of generic data for the ESBWR certification PRA is appropriate for two reasons:

(1) The data are representative of components used in previous BWRs

(2) The specific component brand and/or manufacturer have not been selected.

An evaluation was made of the applicability of the data to the ESBWR components in their specific environments and the values were adjusted as necessary.

19.2.1.5 Human Reliability Analysis

This section describes the methodology applied in evaluating the human interactions (HIs) with the plant systems both during normal operation and during accidents. HIs during normal plant operation are both those that cause an initiating event and those that fail to restore equipment to their normal condition following a test and/or maintenance.

The ESBWR PRA uses a screen approach to human reliability. Operator error probabilities are based on the maximum value expected based on the time available to perform the action. No credit is allowed for improvements based on additional training or special procedures or instructions. Four general time periods are considered for human actions that must occur following an initiating event:

(1) Actions that must be completed within 30 minutes

(2) Actions that must be completed within 60 minutes

(3) Actions that must be completed within 24 hours

(4) Actions that must be completed within 72 hours

No credit is taken for actions in the first category. In general, the failure probability for the other categories are approximately one order of magnitude below the previous.

19.2.2 External Events Analysis

19.2.2.1 Probabilistic Fire Analysis

The Fire Vulnerability Evaluation (FIVE) Methodology developed by the Electric Power Research Institute (EPRI) provides the bases for identifying fire compartments for evaluation purposes, defining fire ignition frequencies, and performing quantitative screening analyses of fire risk. The criterion for screening acceptability is that the risk of core damage from any postulated fire be less than an acceptably small criterion. Any fire scenarios not meeting this criterion require more detailed modeling.

Six scenarios are defined as a function of the building characteristics and the potential damage that could be caused by a fire in each case. The fire frequency is determined for each case, using as a reference the information provided by the FIVE Methodology.

(1) Class 1E DCIS areas in the control building (4 divisional areas)

(2) Reactor building (4 class 1E divisional and 2 non-divisional areas)

(3) Fuel building (1 bounding area)

(4) Turbine building (1 bounding area)

(5) Control room (1 area)

In each of the screening cases, a fire ignition frequency is estimated using the FIVE tables. The fire is assumed to grow unchecked. All of the equipment in the fire area, along with other components in the same electrical division, is assumed to be damaged. A conditional core damage probability is calculated using the appropriate internal event sequence definitions.

The results from this conservative screening analysis show that all the screening cases analyzed have a CDF much lower than the internal events CDF and therefore do not require a further detailed fire analysis. The following insights are provided on the fire mitigation capability of the ESBWR:

(1) Safety system redundancy and physical separation by fire barriers ensure that one fire limits damage to one safety system division. PIP system commonality is limited and is only affected by a few fire areas.

(2) Fires in the control room have the capacity to affect the execution of human actions. One feature relevant to the design is that a fire in the control room does not affect the automatic actuations of the safety systems. The remote shutdown panels allow the mitigation of any accident condition as if the main control room was available.

19.2.2.2 Flooding Analysis

The objective of the ESBWR internal probabilistic flood analysis is to identify and provide a quantitative assessment of the core damage frequency due to internal flood events. Internal floods may be caused by large leaks due to rupture or cracking of pipes, piping components, or water containers such as storage tanks. Other possible flooding causes are the operation of fire protection equipment and human errors during maintenance. The spraying or dripping of water from high-energy pipe breaks or fire protection equipment onto safety equipment is also considered in the analysis. The internal flooding event may contribute to core damage frequency by:

- Initiating an accident sequence which in combination with the probability of random failure events could lead to core damage, and/or
- Disabling safety equipment required to achieve safe plant shutdown

Both types of contributions are considered in the evaluation of internal flooding in buildings that have safety system equipment or Plant Investment Protection systems.

The buildings included in the analysis scope are:

- Reactor Building
- Control Building
- Fuel Building
- Turbine Building
- Electrical Building
- Service Water Building

Flooding scenarios identify potential sources of flooding as well as design characteristics for the mitigation of the consequences of flooding, such as automatic flood detection systems, automatic systems to isolate or end flooding, watertight doors to prevent the progression of the flooding, and other design or construction characteristics that contribute to the minimization of the consequences of flooding.

Core damage frequency is determined as a product of the frequency of each sequence of flood progression multiplied by the conditional probability of core damage for each of them.

The following conservative simplifying assumptions are used to construct and quantify the event trees:

(1) The worst case flooding event in a given building is assumed.

(2) When a flooding event progresses to fail equipment in a safety division, the complete division is assumed to have failed

(3) A scram or plant shutdown is assumed to occur

(4) Given the failures a conditional probability of core damage is calculated. This conditional probability of core damage is evaluated using the ESBWR full power PRA model

The results of the ESBWR bounding analysis show that the CDF for internal flooding is considerably less than the total plant CDF. The risk from internal flooding is acceptably low.

The following insights concerning the flooding mitigation capability of the ESBWR are identified:

(1) Safety system redundancy and physical separation for flooding by large water sources along with alternate safe shutdown features in buildings separated from flooding of safety systems give the ESBWR significant flooding mitigation capability

(2) A small number of location-specific design features must be relied on to mitigate all potential flood sources. The flood specific features are: watertight doors on the Control and Reactor Buildings, floor drains in the Reactor and Control Buildings, Circulating Water System (CIRC) pump trip and valve closure on high water level in the condenser pit

(3) While timely operator action can limit potential flood damage, all postulated floods can be adequately mitigated (from a risk perspective) without operator action

19.2.2.3 High Wind Risk

A previous EPRI assessment of all of the external events identified in the PRA Procedures Guide (Reference 19.2-13) concluded that events other than tornado and earthquake are not considered to be important contributors to ALWR core damage. This is considered to be fully applicable to the ESBWR design.

This section discusses the assessment of the tornado risk following the same approach applied in the ABWR Probabilistic Risk Assessment and presents the results of the ESBWR tornado strike evaluation (Reference 19.2-14).

The loss of offsite power (LOPP) event trees were evaluated using the ARSAP maximum assessed regional value of the expected tornado strike frequency as the loss of offsite power initiating event frequency. In addition, these trees were adjusted to be consistent with the following assumptions resulting from the ARSAP evaluation of the expected ALWR tornado strike vulnerabilities:

- The condensate storage tank and condenser are vulnerable to tornado effects and no credit was taken for either
- Power conversion and feedwater systems are assumed unavailable due to loss of offsite power
- Offsite power recovery is not credited within 24 hours following a tornado strike

The remaining assumptions and conditions for evaluating the loss of offsite power and station blackout event trees for tornado site strike consequences are the same as those documented for LOPP events.

Evaluation of these event trees on the conservative basis listed above yields an extremely small total core damage frequency due to tornado-initiated events compared to the internal event results and the core damage frequency goal. Because tornado-induced events are expected to be such small contributors to core damage frequency, this high-level evaluation was judged to be sufficient and a more detailed analysis is not warranted.

19.2.2.4 Seismic Analysis

A seismic PRA requires site specific details in order for the evaluation to be considered realistic and a best estimate. At the time of certification, only bounding site characteristics are known. A seismic margins analysis was performed to assess the seismic capacities for selected structures and components that have been identified as potentially important to the ESBWR standard plant. The seismic capabilities in terms of seismic fragilities are first estimated, from which the high confidence low probability of failure (HCLPF) capacities are then derived. The HCLPF capacities serve as input to the systems analysis using the seismic margins approach.

The peak ground acceleration of the design earthquakes is 0.3g for the Safe Shutdown Earthquake (SSE). The standard plant designed to these site-envelope seismic loads may result in significant design margins when it is situated at a specific site, particularly a soft soil site. Thus, the seismic capacities estimated from the site-envelope design requirements may be very conservative for certain sites.

For the seismic category I structures and components for which seismic design information is available, the seismic fragilities are evaluated using the factor of safety approach, which is called the Zion method in NUREG/CR-2300 (Reference 19.2-12), PRA Procedures Guide. This approach identifies various conservatisms and associated uncertainties introduced in the seismic design process and provides a probabilistic estimate of the earthquake level required to fail a structure or component in a postulated failure mode by linear extrapolation of the design information supplemented by judgment.

For certain safety-related components such as pumps, valves, and electrical equipment whose design details are not currently available, the generic seismic fragilities recommended in the EPRI ALWR Requirements Document, Appendix A (Reference 19.2-2) or other data sources are used as appropriate. Those generic fragilities are chosen based on a review of prior PRAs and fragility data. They are considered achievable for the ESBWR with an evolutionary improvement in the seismic capacities of the components designed to a 0.3g SSE.

A seismic margins analysis (SMA) is presented for the ESBWR using a modification of the Fragility Analysis method to calculate high confidence low probability of failure (HCLPF) accelerations for important accident sequences and accident classes.

The seismic margins analysis evaluates the capability of the plant and equipment to withstand a large earthquake of 2 times the safe shutdown earthquake (2*SSE).

The HCLPF value of accident sequences obtained from the min-max analysis shows that no accident sequence has a HCLPF lower than 0.60g.

19.2.3 Shutdown Risk Analysis

19.2.3.1 Scope

A detailed Probabilistic Risk Assessment (PRA) is performed to determine the core damage frequency during shutdown.

The evaluation encompasses plant operation in shutdown modes. This evaluation addresses conditions for which there is fuel in the reactor pressure vessel. It includes all aspects of the Nuclear Steam Supply System (NSSS), the containment, and all systems that support operation of the NSSS and containment. It does not address events involving fuel handling outside the reactor building or fuel storage in the spent fuel pool.

The scope of the Shutdown PRA is that of a standard internal events Level 1 PRA. The different accident sequences are classified according to the cooling state of the core, the integrity of the containment and the pressure of the containment at the end of the sequence.

A series of boundary plant configurations are defined in order to limit the number of event trees. These configurations are similar with regard to residual heat and mitigation systems behavior and availability. These plant configurations are as follows:

- Mode 3 (hot shutdown)
- Mode 4 (cold shutdown)
- Mode 5 with reactor well unflooded (refueling)
- Mode 5 with reactor well flooded (refueling)
- Mode 1 – 3 for evaluating manual shutdown of the reactor

19.2.3.2 Initiating Events

A shutdown initiating event is defined as any event that provokes a disturbance in the stable state of the plant and that requires some kind of action to prevent damage to the core.

Two shutdown critical safety functions are identified

(1) Decay heat removal

(2) Reactor Coolant System (RCS) inventory control.

Within the decay heat removal function, three initiating events are considered

(1) The loss of Reactor Water Cleanup / Shutdown Cooling System (RWCU/SDC)

(2) The loss of plant cooling systems (Reactor Component Cooling Water System or Plant Service Water System)

(3) The loss of preferred power (LOPP).

These initiating events are evaluated for all the plant configurations except in Mode 5 flooded, as the large water inventory stored above the core in this case is able to assure core cooling for long periods of time even if the decay heat removal system fails.

The frequencies of the initiators related to loss of decay heat removal are estimated either from the dominant failure modes or from industry operational experience.

In the case of RCS inventory control, the following types of scenarios were analyzed:

- Random pipe breaks within the RCS (including breaks related to maintenance or refueling activities)
- Misalignment of systems connected to the RCS
- Leakage during Fine Motion Control Rod Drive replacement

Manual shutdown is also considered as an initiating event in the shutdown analysis.

19.2.3.3 Accident sequences

Unlike full power conditions, extended time can be available to terminate the initiating event. This justifies credit for limited recovery actions.

The recovery events considered are generally those that terminate the initiating event before the plant reaches a state challenging a safety function. The following recovery events are analyzed:

- Loss of both operating RWCU/SDCS trains. The operator can recover one of the two failed trains.
- Loss of Preferred Power. A power recovery event is possible due to operator or external actions.
- Loss of RCCWS/PSWS. The operator can recover the failed equipment.
- LOCA (reactor vessel head removed). The operator can close the two lower drywell hatches if they are open.

The analysis of these recovery events is performed using industry data over selected operating experience periods.

The end states of the accident sequences are the same as in the full power PRA.

During mode 5, when the containment is open, sequences leading to core melt are designated as CD V.

19.2.3.4 Shutdown PRA Results

The greatest contribution to shutdown risk comes from breaks in lines connected to the vessel below TAF that occur in mode 5. In this mode, the lower drywell equipment hatch or personnel hatch is likely to be open to facilitate work in the lower drywell. This accident can only be terminated by closing the hatch(es).

In order to minimize the risk from these scenarios, refueling outages must be conducted in a judicious manner. Whenever the hatches are open, procedures shall require personnel to be available and in close proximity to the hatches, with the purpose of providing fast closure of the containment in the case of a water leak.

Other measures can be taken, including temporarily install equipment to aid in closing the hatch or to minimize the flooding rate in the lower drywell.

The other significant contribution to shutdown risk comes from the loss of preferred power initiating event. This is a slow moving event because of the mass of water needed to boil away prior to core damage. Thermal-hydraulic calculations show that the core will not begin to uncover before approximately 23 hours following the loss of power. It is expected that recovery of offsite power will enable the operators to provide injection to reflood the core.

19.2.4 Containment Performance Analysis

The response of the RPV and the containment during severe accidents is analyzed in NEDC-33201. Postulated severe accident sequences are selected such that both the core damage accident classes and the key aspects of the containment response are represented. The severe accident sequences which were evaluated for detailed modeling represent more than 99% of the core damage frequency (CDF) identified by the Level 1 PRA. In addition, scenarios with very low frequencies of occurrence, much lower than dominant contributors to the CDF, are also treated to account for phenomenological and analytical uncertainties. These are considered residual risk, as described later in this section.

Systems Considered in Containment Performance Analysis

- The systems considered in the containment performance analysis are listed below. GDCS In-Vessel Injection
- GDCS Deluge/BiMAC Operation
- Containment Heat Removal (PCCS only)

  Containment heat removal can be provided by either the PCCS or the suppression pool-cooling mode of the FAPCS. For sequences with successful containment heat removal, the thermal-hydraulic analysis assumes that the PCCS is available and suppression pool cooling is not. This assumption bounds containment pressure response because the PCCS can only limit pressurization, while suppression pool cooling can limit and reduce containment pressure.
- Vacuum Breakers
- Suppression Chamber Vent

Recovery of failed systems is conservatively considered not to occur during the 72-hour post-accident time period that is considered in the containment performance analysis.

Operator Actions in Severe Accident Analysis

The only operator action credited in the level 2 is venting through the suppression chamber to prevent containment overpressurization. This is only included in the scenarios where the passive containment protection features are failed. It is assumed that venting would occur only if containment pressure reached 90% of the ultimate pressure capability.

Containment Release Modes

Section 19.3 discusses the potential for containment failure due to direct containment heating, ex-vessel steam explosion and basemat penetration. In the absence of one of those energetic and potentially early containment failure modes, the three modes of fission product release from containment listed below remain for consideration in the containment performance analysis:

(1) Technical Specification Leakage

(2) Drywell Failure

(3) Containment Venting

Accident Termination Time

The containment challenge scenarios are terminated at 72 hours. Operator action prior to the expiration of 72 hours is considered to be highly likely.

Residual Risk

The sequences that make up more than 99% of CDF are analyzed in the level 2 analysis based on their effect on containment performance. To account for analytical or phenomenological uncertainties, an additional sequence is evaluated to account for unknown contributions to the source term for the consequence analysis. These are all treated as containment bypass scenarios.

19.2.5 Offsite Consequences Analysis

This subsection summarizes the PRA offsite consequence evaluation. Key inputs and assumptions are described and the calculated results are compared to consequence related goals to show that the goals are satisfied. Details of this analysis are provided in Section 10 of NEDC-33201 (Reference 19.2-14) and related references 19.2-15 to 19.2-26.

19.2.5.1 Method

Offsite dose and consequences for each source term (i.e., radionuclide release category) are evaluated over a range of possible weather conditions and evacuation assumptions. ESBWR specific reference data from the PRA level 2 plant performance analysis are used as input for the source term.

19.2.5.1.1 Site Assumptions

The evaluation of the offsite consequences of a reactor accident are closely tied to the site parameters (e.g., weather, population, land use). For probabilistic offsite consequence evaluations, site related assumptions are required. The subsections below describe the rationale for the site meteorology, population, and evacuation.

19.2.5.1.2 Meteorology

The ALWR URD meteorological reference data set is used, which is indicative of meteorological data significantly worse than the average U.S. site. Therefore, the results in this study represent a generally bounding evaluation for most U.S. sites.

19.2.5.1.3 Population

For the ESBWR consequence evaluation, the SANDIA Siting Study population density table (Section 10 of NEDC-33201) is used to develop a uniform population density corresponding to each spatial interval. The population distribution is developed for distances to 0.5, 1, 2, 3, 4, 5, 10, 20, 30, 40 and 50 miles from the site.

19.2.5.1.4 Evacuation

Many evacuation related characteristics (local roads, population demographics, emergency services) are quite site specific. The NRC gives no general guidance for generic evacuation evaluations. The evacuation parameters used in this study are conservative assumptions in that no evacuation or relocation in terms of physical movement is assumed and no sheltering is assumed. The public is assumed to continue normal activity during the reactor accident in this bounding analysis. Shielding and exposure values used for normal activity are also assumed.

19.2.5.2 Radionuclide Release Input Data

ESBWR specific radionuclide release data is used in this analysis to model the dispersion of a plume of material released to the environment during a reactor accident. The inputs are:

- Building Data for Meteorological Modeling of Wake Effects
- Core Inventory Parameters
- Reactor Accident Release Parameters
- Nuclide Release Categories

The input data is provided from the severe accident progression analysis discussed in Section 19.2.4. The detailed consequence analysis input data is provided in Sections 8 and 9 of NEDC-22301.

ESBWR specific parameters are used for wake effect data, core inventory, and reactor thermal power. The width and height of the building wake are used to model the initial plume dimensions. The core inventory and reactor thermal power used in this analysis are ESBWR specific and are used to determine the inventory of each nuclide in the core at accident initiation.

The four source terms used for the consequence analysis are based upon the following release categories:

(1) Break Outside Containment (BOC)

(2) Core Concrete Interaction – Dry (CCID)

(3) Filtered Release (FR)

(4) Technical Specification Leakage (TSL)

For each source term, the release is modeled to occur at ground level. The thermal content of each release is assumed to be the same as ambient (i.e., buoyant plume rise is not modeled). This is conservative for early fatalities as discussed in Section 10 of NEDC-33201.

19.2.6 References

19.2-1 NUREG/CR-5750, Rates of Initiating Events at U.S. Nuclear Power Plants: 1987-1995, December 1998.

19.2-2 Advanced Light Water Reactor Utility Requirements Document, Volume II, ALWR Evolutionary Plant, Chapter 1, Appendix A, PRA Key Assumptions and Groundrules, EPRI, 1990.

19.2-3 ABWR PRA Advanced Boiling Water Reactor Standard Safety Analysis Report, GE Nuclear Energy, 23A6100. Rev. 9, August 1996.

19.2-4 NUREG/CR-5497, Common-Cause Failure Parameter Estimations, October 1998.

19.2-5 EPRI-TR-100382, A Database of Common-Cause Events for Risk and Reliability Applications, June 1992.

19.2-6 NUREG/CR-5801, Procedure for Analysis of Common-Cause Failures in Probabilistic Safety Analysis, April 1993.

19.2-7 NUREG/CR-4780, Procedures for Treating Common-Cause Failures in Safety and Reliability Studies, January 1988.

19.2-8 EPRI NP-3583, Systematic Human Action Reliability Procedure (SHARP), June 1984.

19.2-9 NUREG/CR-1278, Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plants Applications Final Report, August 1983.

19.2-10 NUREG/CR-4772, Accident Sequence Evaluation Program – Human Reliability Analysis Procedure, February 1987.

19.2-11 “Fire Vulnerability Evaluation Methodology, FIVE, Plant Screening Guide”, Electric Power Research Institute, September 26, 1991.

19.2-12 NUREG/CR-2300, PRA Procedures Guide, January 1983.

19.2-13 EPRI NP-2005, Tornado Missile Simulation and Design Methodology, Volumes 1 & 2, August 1981.

19.2-14 GE Nuclear Energy, “ESBWR Design Certification Probabilistic Risk Assessment” NEDC-33201, September 2005

19.2-15 Chanin, D. and Young, M., Code Manual for MACCS2: User’s Guide, NUREG/CR-6613, Vol. 1 (SAND97-0594), May 1998.

19.2-16 Murley, T.E., Advanced Boiling Water Reactor Licensing Review Bases, Project No. 671, August 7, 1987.

19.2-17 “MAAP4 Modular Accident Analysis Program for LWR Power Plants,” Transmittal Document for MAAP4 Code Revision MAAP 4.0.6, Rev. 0, Report Number FAI/05-47, prepared for Electric Power Research Institute, 05/05/05.

19.2-18 “SBWR SSAR” Section 19.B.4.2.

19.2-19 “ABWR SSAR”, Section 19.E.2.

19.2-20 Chanin, D. and Young, M., Code Manual for MACCS2: User's Guide, NUREG/CR-6613, Vol. 1 (SAND97-0594), May 1998.

19.2-21 Spring, J.L. et al, Evaluation of Severe Accident Risks: Quantification of Major Input Parameters, MACCS Input NUREG/CR-4551, December 1990.

19.2-22 Reactor Safety Study, Appendix 6: Calculation of Reactor Accident Consequences, WASH-1400 (NUREG 75/014), October 1975.

19.2-23 Aldrich, D.C., et al, Technical Guidance for Siting Criteria Development NUREG/CR-2239, December 1982.

19.2-24 Criteria for preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, NUREG-0654.

19.2-25 Murley, T.E., Advanced Boiling Water Reactor Licensing Review Bases, Project No. 671, August 7, 1987.

19.2-26 1986 Cancer Facts and Figures, American Cancer Society, 90 Park Ave, New York, NY 10016.

Table 19.2-1

Systems and Functions Modeled

Report	Functions Modeled
Reactor Depressurization System Analysis	Depressurization (SRV or DPV) Overpressure Protection Containment Isolation
Isolation Condenser System Analysis	Reactor Heat Removal Containment Isolation
Control Rod Drive System Analysis	RPV Injection at High Pressure
Standby Liquid Control System Analysis	Boron Injection
Instrument and Control System Analysis	Non-Safety Related Multiplexing Non-Safety Related Signals ADS Inhibit Feedwater Runback RPV Isolation Safety Related Multiplexing Safety Related Signals
Gravity Driven Cooling System Analysis	RPV Short/Long Term Low Pressure Injection Injection from Equalizing Lines
Fuel & Auxiliary Pool Cooling System Analysis	Suppression Pool Cooling Low Pressure Coolant Injection IC/PCC Pool Makeup from Fire Water RPV Injection from Fire Water
Reactor Water Cleanup & Shutdown System Analysis	Shutdown Cooling Containment Isolation

Table 19.2-1

Systems and Functions Modeled

Report	Functions Modeled
Feedwater and Condensate System Analysis	RPV Injection at High Pressure Containment Isolation BOP Heat Sink Component Cooling
Reactor Component Cooling Water System Analysis	Reactor Building Component Cooling
Plant Service Water System Analysis	Component Cooling Ultimate Heat Sink
Instrument Air System (IAS) Service Air System (SAS) Analysis	Valve Motive Power Valve Motive Power
High Pressure Nitrogen Supply System Analysis	Valve Motive Power
AC Power Distribution System Analysis Uninterruptible AC Power System Analysis 250 Vdc Power System Analysis	AC Power Onsite AC Power Uninterruptible AC Power DC Power
Containment System Analysis	Containment Vent Containment Isolation
Passive Containment Cooling System Analysis	Containment Ultimate Heat Sink

19.3 SEVERE ACCIDENT MANAGEMENT

19.3.1 Overview of ESBWR Severe Accident Design Features

The Level 1 PRA results show that core damage events (Severe Accidents) in the ESBWR which may challenge containment integrity are very low probability occurrences. Still design features and procedures have been developed that provide an additional (diverse and redundant) layer of defense against all threats to containment integrity that such hypothetical events may conceivably entail.

Given a severe accident, threats to containment integrity may be enumerated as follows:

- *Prompt, Energetic Loading*: extensive fuel-coolant interactions, high-pressure melt ejection leading to direct containment heating (and pressurization),
- *Late, Gradual Loading*: melt ablation and penetration of the containment basemat, pressurization of containment atmosphere by steam and/or non-condensable gases, and
- *Isolation Failure*: errors or malfunctions that leave existing flow paths open to the outside, activation of the containment overpressure protection system.

This section deals with the phenomenological components of these threats; namely, Ex-vessel Steam Explosions (EVE), Direct Containment Heating (DCH), and Basemat Melt Penetration (BMP). Table 19.3.1-1 summarizes the Abbreviations and Acronyms used in Section 19.3.

The ESBWR Severe Accident Management (SAM) strategy is based upon arresting the melt propagation process and ensuring long term coolability within the containment boundary. It was determined that the ex-vessel behavior could be managed so that coolability could be addressed ex-vessel with a high degree of certainty. Thus ex-vessel behavior is the principal focus of the treatment in this section. Manifestations of the above threats are addressed in a manner that is inclusive of all possible ex-vessel evolutions.

The ESBWR features inerting of the containment atmosphere with nitrogen and maintaining a slightly positive pressure to prevent air in-leaking into the containment to prevent deflagration or detonation of combustibles. A drywell spray system is provided to support accident recovery operations. Unlike the ABWR, or any other previous GE BWR, the ESBWR containment design includes the Passive Containment Cooling System (PCCS) to remove decay heat from the containment, and the (also passive) Basemat-Internal Melt Arrest and Coolability (BiMAC) device to essentially eliminate the possibility of extended corium-melt interactions, non-condensable gas generation, and base-mat penetration. In addition the ESBWR is equipped with an Isolation Condenser System (ICS), a natural circulation system for decay heat removal from the RPV, especially in sequences that failed to depressurize. A manual containment venting capability (MCOPS) is included to prevent containment failure by overpressurization. This system is designed to open and re-close under severe accident pressure conditions.

An overall illustration that summarizes all of these systems in the framework of the ESBWR containment can be found in Figure 19.3.1-1. From top down: (i) PCCS pool and heat exchangers provide passive containment cooling; (ii) ICS pool and heat exchangers provide natural circulation decay heat removal from RPV; (iii) GDCS (three pools, four divisions) with ADS (DPV, SRV) makes up the ECCS; GDCS deluge line supplies BiMAC for long-term coolability; (iv) MCOPS provides manual venting from the wetwell in a controlled manner; (v)

Basemat-Internal Melt Arrest and Coolability (BiMAC) device (shown in the bottom insert) is initially fed by water flow from squib-valve-operated GDCS deluge lines into a distributor channel, and through a pipe jacket (with inclined and vertical portions) into the LDW cavity. The cooling in a later phase is provided by natural circulation of water in the LDW feeding into the distributor channel through downcomers (at the end of LDW, not shown in the insert). For more details, see Section 19.3.5 (BMP).

The ESBWR certification PRA report NEDO-33201 contains detailed description of the severe accident treatment for the ESBWR.

19.3.1.1 References

19.3.1-1 T.G. Theofanous, C. Liu, S. Additon, S. Angelini, O. Kym¨al¨ainen and T. Salmassi (1996), “In-Vessel Coolability and Retention of a Core Melt,” DOE/ID-10460, Vols. 1 and 2, October 1996.

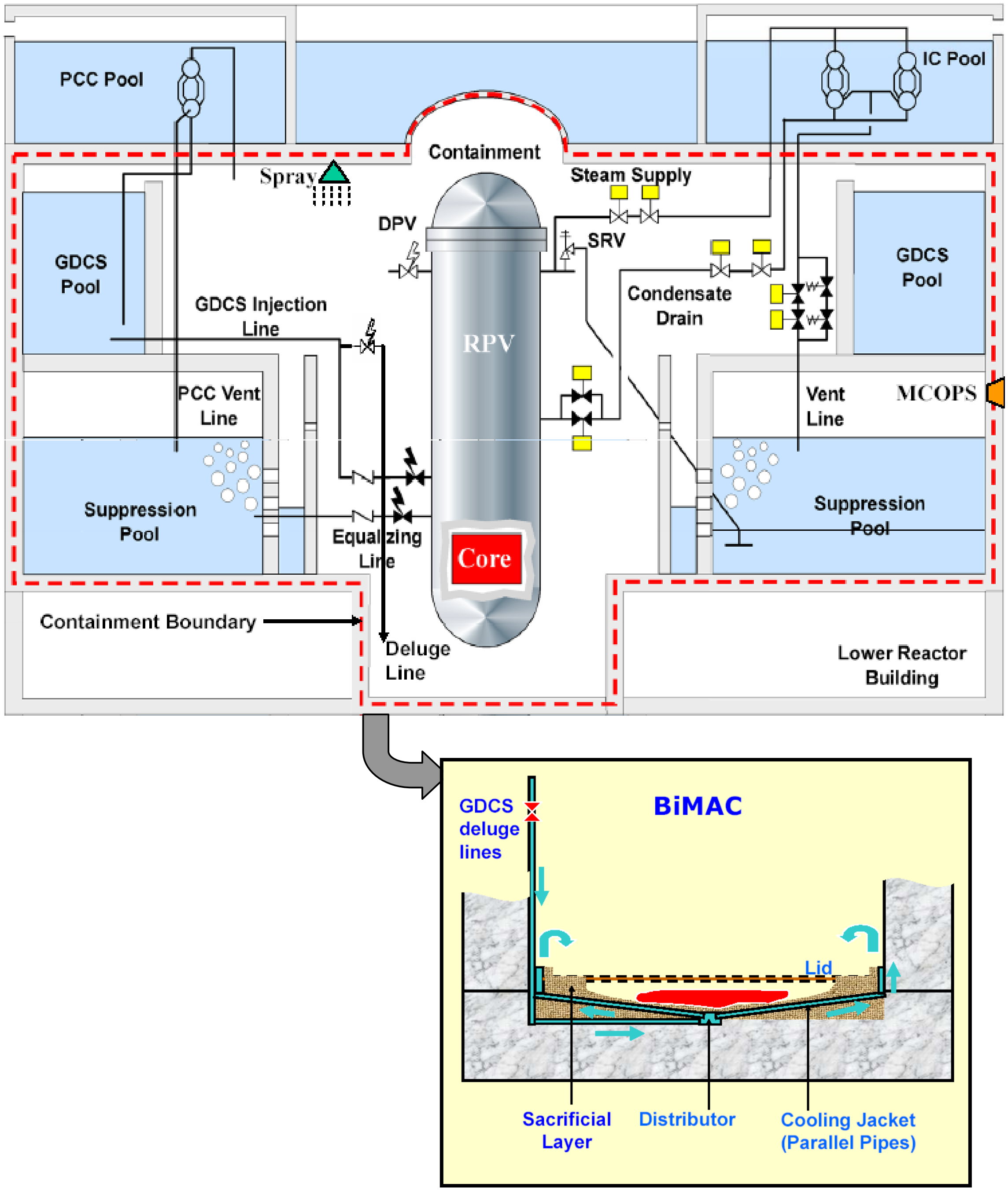


Figure 19.3.1-1. Summary of the ESBWR Severe Accident Design Features

19.3.2 Overall Severe Accident Assessment Methodology

The Risk Oriented Accident Analysis Methodology (ROAAM) was developed for the purpose of resolving "issues" that proved hard to address in a purely probabilistic (PRA) framework. This purpose was met mainly due to a methodological emphasis on deterministic principles of key physics along with an overall conservative approach of treatment (Theofanous, 1996). The principal ingredients of ROAAM include: (a) identification, separate treatment, and maintenance of this separation (to the end results), of Aleatory and Epistemic uncertainties; (b) identification and bounding/conservative treatment of Intangibles and Splinters; that is of epistemic uncertainties (in parameters and scenarios respectively) that are beyond the reach of any reasonably verifiable quantification; and (c) the use of external experts in a review, rather than in a quantification capacity.

Under the auspices of the US NRC so-resolved issues include: "Mark-I Liner Attack" (Theofanous et al, 1991), "Direct Containment Heating for PWRs" (Pilch, Yan and Theofanous, 1994), and, in a preliminary rendition, "Alpha Mode Failure for PWRs" (Theofanous et al, 1987). Under support from the US DOE's ARSAP program the innovative In-Vessel Retention (IVR) technology for Westinghouse's AP600 and AP1000 designs was developed and assessed (Theofanous et al 1996; Scobel, Theofanous and Sorrell,1998) , as was an early version of severe accident treatment for GE's SBWR (Theofanous, 1993c). The present treatment for ESBWR is based on the same philosophy of approach, same overall methodology, and it leverages on ideas, data, and tools developed during all this past work.

The principal consideration in addressing ex-vessel behavior is whether the lower head fails with the RPV being at high or low pressure (HP vs. LP). The demarcation is provided by the capacity of the resulting (superheated steam) blowdown to disperse previously ejected debris into the upper drywell (UDW), and conservatively we take this here to be at 1 MPa (see Section 19.3.3 on DCH). Thus, as a simplified overview, we have the frame in which two potential containment threatening events manifest themselves: direct containment heating (DCH) for HP events, and basemat melt penetration (BMP) for LP sequences as well as for HP sequences because a portion of the debris exits after the RPV has been depressurized. The other fundamental measure of ex-vessel behavior concerns the amount and temperature of water present on the lower drywell (LDW) floor at the time of vessel failure. This defines the potential extent and severity of steam explosions. In addition to the usual pedestal integrity concern, here we need to also consider the potential impact on the continued functioning of the BiMAC device.

A selection of ESBWR severe accidents, as derived from Level-1 PRA results, is shown in Figure 19.3.2-1. Sequences with failure of the RPV pressure boundary at low pressure (<1 MPa) belong to Class I accident sequences. Sequences with core cooling successful at the time of containment failure, but cooling lost as a result of containment failure belong to Class II. Sequences with failure of the RPV pressure boundary at high pressure (>1 MPa) belong to Class III accident sequences. Sequences with failure to insert negative reactivity such as Anticipated Transient Without Scram (ATWS) belong to Class IV accident sequences. Sequences involving containment bypass belong to Class V accident sequences. The severe accidents in ESBWR Class II can be ignored because these sequences do not fail the core until after 72 hours and are recoverable with manual actions. Thus, DCH, EVE, and BMP are not applicable to Class II. The EVE is not applicable to Class III because the LDW has only a small amount of condensate in all such sequences. The DCH is not applicable to Class I. The BMP is of concern to all severe accident sequences. The intent is to illustrate how the CDF is attributed to various kinds of Severe Accident (SA) sequences, along with the kind of containment integrity considerations appropriate to each case. First we note that the main contributors to CDF are the Class I (LP) and Class III (HP) scenarios. The detailed decomposition of the CDF into classes is provided in Section 19.2.

DCH is only relevant to High Pressure Class III, while EVE is relevant to Low Pressure Class I. Of the HP sequences, no containment spray available constitutes the limiting condition for the DCH thermal loads. Of the LP sequences, flooded LDW to what we have defined as a high level in the LDW constitutes the limiting condition for pedestal and BiMAC failure under steam explosion loads. Finally, the BMP is an all-encompassing issue.

The ROAAM treatment consists of five basic steps:

- **Identification of the Key Physics.** This includes the definition of all principal mechanisms, their potential interactions, and order of magnitude estimations that we use in defining an optimal approach for quantifying how loads (thermal and/or mechanical) compare to failure behaviors (fragilities).
- **Definition of a Probabilistic Framework.** This is to define the model(s) for the overall mechanics of quantifying loads, fragilities, and probabilities of failure. In particular this shows the decomposition employed, types of uncertainties involved (in this decomposition), and the treatment of these uncertainties in the quantification.
- **Quantification of Loads.** This goes into the technical details of quantifying loads with the intent of enveloping uncertainties. Also covered are the bases for the models used, and evidence of their verification/validation status.
- **Quantification of Fragilities.** This addresses failure criteria, and in particular the intent is to provide a solid quantification of failure incipience (conservatively) and at the other extreme of gross failure.
- **Quantification of Failure Probabilities.** With all the above at hand, in this step we simply employ the probabilistic framework to calculate failure probabilities.

To complete the ROAAM process, GE internal and external experts conducted an independent review of the severe accident treatment. The results of their review is included in NECO-33201.

19.3.2.1 References

19.3.2-1 T.G. Theofanous, W.H. Amarasooriya, H. Yan and U. Ratnam (1991), "The Probability of Liner Failure in a Mark-I Containment," NUREG/CR-5423, August 1991.

19.3.2-2 T.G. Theofanous, H. Yan/UCSB; M.Z. Podowski, C.S. Cho/RPI; D.A. Powers, T.J. Heames/SNL; J.J. Sienicki, C.C. Chu, B.W. Spencer/ANL; J.C. Castro, Y.R. Rashid, R.A. Dameron, J.S. Maxwell, D.A. Powers/ANATECH (1993a), "The Probability of Mark-I Containment Failure by Melt-Attack of the Liner," NUREG/CR-6025, November 1993.

19.3.2-3 M.M. Pilch, H. Yan and T.G. Theofanous (1994), "The Probability of Containment Failure by Direct Containment Heating in Zion," NUREG/CR-6075, SAND93-1535, December 1994. M.M. Pilch, H. Yan and T.G. Theofanous, “The Probability of Containment Failure by Direct Containment Heating in Zion,” *Nuclear Engineering & Design*, 164 (1996) 1–36.

19.3.2-4 T.G. Theofanous, B. Najafi and E. Rumble (1987), “An Assessment of Steam-Explosion-Induced Containment Failure. Part I: Probabilistic Aspects,” *Nuclear Science and Engineering*, 97, 259-281 (1987). M.A. Abolfadl and T.G. Theofanous, “An Assessment of Steam-Explosion-Induced Containment Failure. Part II: Premixing Limits,” *Nuclear Science and Engineering*, 97, 282-295 (1987). W. H. Amarasooriya and T.G. Theofanous, “An Assessment of Steam-Explosion-Induced Containment Failure. Part III: Expansion and Energy Partition,” *Nuclear Science and Engineering*, 97, 296-315 (1987). G.E. Lucas, W.H. Amarasooriya and T.G. Theofanous, “An Assessment of Steam-Explosion-Induced Containment Failure. Part IV: Impact Mechanics, Dissipation and Vessel Head Failure,” *Nuclear Science and Engineering*, 97, 316-326 (1987).

19.3.2-5 J.H. Scobel, T.G. Theofanous and S.W. Sorrell (1998), “Application of the Risk Oriented Accident Analysis Methodology (ROAAM) to Severe Accident Management in the AP600 Advanced Light Water Reactor,” *Reliability Engineering and Safety Systems*, 62 (1998) 51-58.

19.3.2-6 T.G. Theofanous (1993c) “Ex-Vessel Coolability for the SBWR”, Report to DOE/ARSAP (ANL). August 5, 1993.

19.3.2-7 NEDC-33201 GE’s ESBWR Certification PRA Report, (2005)

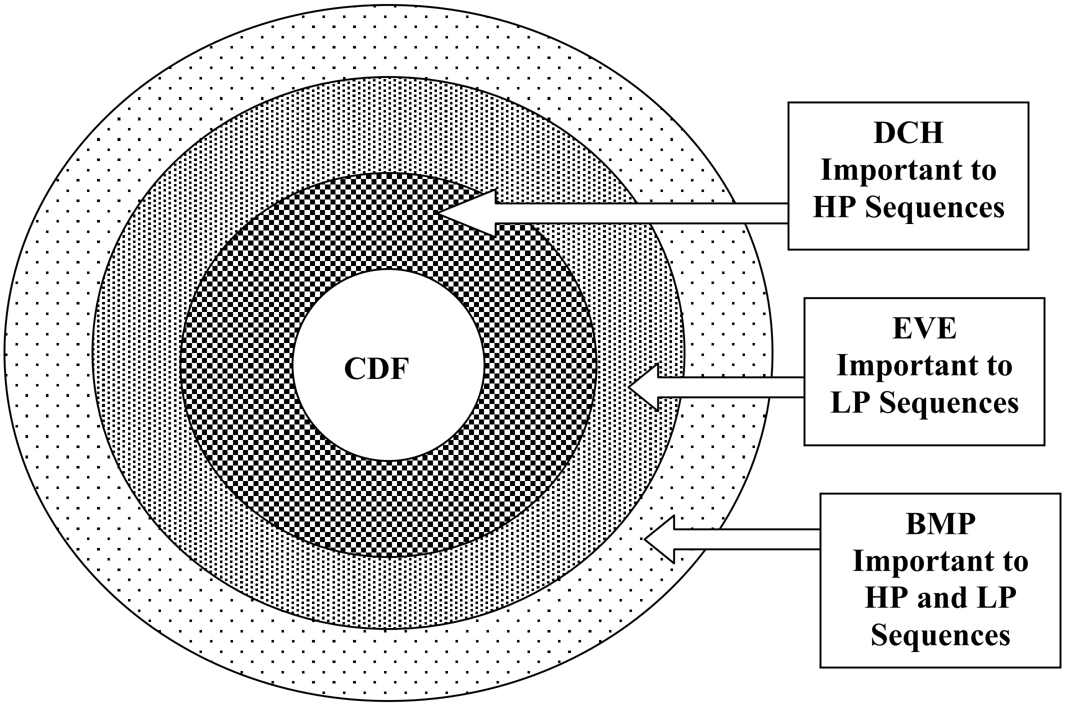


Figure 19.3.2-1. Severe Accident Phenomenology and CDF in ESBWR

19.3.3 Direct Containment Heating (DCH)

19.3.3.1 Overall Considerations

The set of accidents that lead to DCH consists of those involving core degradation and vessel failure at high primary system pressure. A necessary condition for this is that a minimum of 2 out the 4 isolation condensers have failed due to either water depletion on the secondary side, or due to failure to open the condensate return valves that keep these IC's isolated during normal operation. In addition, all 8 reactor depressurization valves (DPV), and all 18 of the Safety Relief Valves (SRV) must fail to operate. The probability of such combinations of events is extremely low, and accordingly for the ESBWR, such events must be thought of as *remote and speculative; that is, they could be left in the category of residual risks* (Theofanous, 1996, Scobel, Theofanous, and Sorrell, 1998). Moreover, as in PWR HP scenarios (Pilch, Yan, and Theofanous, 1994), natural convection, and forced flow due to SRV lifting, could be sufficient to thermally load the relief lines to failure, thus producing "natural depressurization", and transition to Low Pressure (LP) scenario (prior to lower head breech by the relocated molten core debris). Still, due its potentially severe consequences, we choose to examine the potential for energetic containment failure due to DCH, and show that such a failure is *physically unreasonable*.

The key ingredient towards such a conclusion is that the vent area, connecting to the enormous condensation potential of the suppression pool, makes it virtually impossible to pressurize the drywell volume.

19.3.3.2 ESBWR Design

An overall illustration of the ESBWR drywell, with highlights on features that impact DCH loading is given in Figure 19.3.3-1. The relevance of each of these features can be summarized as follows:

a. Initially the vents are covered with water, so the DW volume must be considered closed for as long as it would take to force this water out under the action of DCH (addition of gaseous mass and energy) on the UDW atmosphere. Thus the initial supply rate is critical, and just as in a LOCA this vent-clearing defines the peak pressure attainable in such an event. For pressurization levels of interest to DW integrity, this vent-clearing time is something under 1 s.

b. The pathway that connects the LDW to the UDW is an annular space around the RPV with a characteristic dimension of ~ 2 m. As illustrated, in the LDW region this path is partially occupied by the reflective insulation that surrounds the RPV. Assuming that this structure provides minimal resistance to the flow, we, conservatively, ignore its presence. In the UDW region, the path is between the shield wall and the suppression pool wall. At the level of the suppression pool bottom, the path between LDW and UDW is narrowed by 8 massive blocks on which the RPV is supported.

c. The role of the BiMAC cover plate, in addition to providing a base for workers to walk on, is to trap debris released during high pressure melt ejection, and to provide some degree of separation from the high velocity gas flow present during the subsequent blowdown phase.

d. The in-vessel natural convection flow paths redistribute heat during the oxidation and degradation phases of a severe accident to the upper vessel internals, and through the top portions of the upper plenum into the various lines that lead to the SRVs, DPVs, and the IC's.

19.3.3.3 Previous Work

Direct containment heating has been considered to be a major containment integrity issue and this drove very extensive research efforts during the late 80's and early 1990's. These efforts culminated with issue resolution in a ROAAM framework as documented in Pilch, Yan, and Theofanous (1996), and Pilch and Allen (1996).

The principal ingredient in quantifying DCH loads is the realization that oxidation of the reactive components of the melt and heat transfer is limited by the entrainment/dispersal process occurring over a time scale that limits contact to a fraction of the available steam. This expressed as the DCH-scale, namely the ratio between the characteristic melt sweep-out time (τ_m), and blowdown time constant (τ_s), allows us to place upper bounds on the rate of dispersal through application of values found experimentally (0.5 to 2) (Yan and Theofanous, 1996). A comprehensive summary of previous work on DCH is provided in NEDC-33201.

19.3.3.4 Present Assessment

Key Physics in DCH

Direct containment heating can be expected when high velocity steam happens to impinge upon melt already released into a containment compartment, thus creating regions of fine scale mixing, large interfacial area for heat transfer, and oxidation of metallic components in the melt. The so-heated steam, flowing at very high volumetric flow rates, then provides a mass-and-energy source that can pressurize and heat the receiving atmosphere. Concurrently, the finely atomized melt is carried against gravity into the receiving volume(s), where the steam velocities are highly reduced, and the particles are allowed to fall (de-entrain). In ESBWR, the mixing occurs in the LDW, while the main receiving volume, in which de-entrainment occurs, is the UDW. These correspond to the reactor cavity and the sub-compartment(s) of Large Dry Containments (LDC) in PWRs respectively. In distinction to LDCs, in the ESBWR, as in all BWRs, the receiving volume, rather than being closed, is vented to a much larger volume, the WW. This venting occurs through the suppression pool, which is thus intervening by means of a very effective heat sink. The key physics that drive all these phenomena, and that need to be quantified in predicting a realistic outcome, are as follows:

a. **Natural Depressurization and RPV Lower Head Breach.** Natural depressurization, and thus transition to a low-pressure scenario, would occur if any of the SRV, DPV, or IC lines were to fail (due to thermal loading by gas natural convection) prior to breaching (by melt attack) the lower head. Pivotal considerations in this "competition" for failure can be summarized as follows. The relevant time scale is defined by the first major relocation of core debris into the lower plenum. Simple estimates based on core heat capacities, decay power levels, and oxidation energies indicate a time frame of 40 to 70 minutes following core un-covery. The superheating of gases during this time period can lead to temperature levels of ~1000 K in the upper RPV area, and in direct communication with the inlets to the SRV, DPV, and IC lines. The flow of these gases into the SRV lines would be convective, as the valves lift periodically to relieve pressure, and the material temperatures thus-reached would indicate a margin of ~100 K to creep rupture (Smith, 1971, Reddy and Ayers, 1982). On the other hand, in order that DCH occurs to any significant degree we must have a large quantity of melt in a lower plenum that has been mostly depleted of water. This configuration in turn has to have resulted from the re-melting of a previously-quenched debris, a process that would develop from the inside-out, thus eventually reaching a penetration weld, and leading to lower head breach (penetration equipment falling off).

b. **Melt Ejection, Vessel Wall Ablation, and BiMAC Refractory Cover Ablation**: Due to negligible resistance by the LDW atmosphere, the melt jet would remain coherent until it hits the LDW floor, and the BiMAC cover plate, which will be penetrated essentially instantaneously to allow free access to the sacrificial refractory layer that covers and protects the top of the BiMAC pipes. The vessel wall would ablate due to heat transfer from superheated melt. So would the refractory material if melt temperature exceeds its melting point. These processes are well understood and this understanding is supported by experiments. Results depend on the melt composition and superheat which are evaluated in a bounding fashion as intangible parameters. Similarly, the amount of melt-mass ejected, and the mass fractions of Zirconium and Iron in the melt, are treated as intangibles and evaluated in a conservative fashion.

c. **Steam Blowdown**: The steam inside the reactor vessel would expand adiabatically during blowdown, and the steam discharge rate is defined by shocked flow at the vessel breach area(s). Both processes can be accurately simulated by means of simple thermodynamics (ideal gas equation of state, adiabatic expansion) and Computational Fluid Dynamics (CFD) simulations respectively.

d. **Interfacial Instability, Breakup, Entrainment, and Carry-over of Melt Exposed to the Gas Stream Inside the LDW.** Liquids exposed to high velocity gas streams atomize and disperse. The mode and magnitude of the interfacial instability responsible for this behavior depends on the Weber number, which is the ratio of the destabilizing momentum flux of the gas (ρv^2) to the stabilizing surface tension force (σ/R). For corium melt, the surface tension is about 10 times that of water, so the stability limit will be (for the same momentum flux) at a length scale that is ~10 times that of water. For example at a gas velocity of 300 m/s and atmospheric density of 1 kg/m^3, the stable droplet size for water is ~10 microns, and for corium it is ~100 microns. This stability limit is captured by a critical Weber number of ~10. Thus even a relatively small drop of 10 mm will experience an initial We number of 10^3 and a breakup pattern such as that the mist shown would be at ~100 rather than ~10 microns.

Melt particles of 100 microns size can be suspended by air/steam velocities of as low as ~ 0.3 m/s. In addition, pressure induces macroscopic motions that accelerate bigger masses of liquid up the pedestal walls. Any exposed melt inside the LDW will be atomized and dispersed into the UDW. Much of it would then be carried into the suppression pool, while some fraction would de-entrain and deposit on the UDW walls or fall on the floor, in a highly dispersed state.

e. **Entrainment of Melt Captured inside the BiMAC.** While the pressure established inside the BiMAC is the same as the stagnation pressure on the top of the cover plate due to high frequency flow fluctuations, these pressures are unsteady. A net circulation pattern is established that continuously brings liquid into the immediate vicinity of the opening from where it is entrained to the outside in a highly atomized form. The velocities in this region can be high. The mass loading on the flow is rather low so the Weber numbers may approach 10^4 and the length scales of atomization may be as low as 10 micron. Such particles could be carried around by gas flows as low as 0.3 m/s. The NEDC-33201 report provides more detailed evaluation of the process.

19.3.3.5 Summary and Conclusions for DCH

The detailed probabilistic framework, quantification of DCH loads, quantification of fragility to DCH, and prediction of failure probability due to DCH are described in the GE PRA report NEDC-33201. The results described in NEDC-33201 show that the ESBWR containment can withstand bounding DCH loads and containment failure due to DCH is physically unreasonable.

Principal ingredients to such a conclusion can be summarized as follows:

- Large vent area from the UDW into a huge heat sink of the WW,
- An effectively isolated Drywell Head from the UDW atmosphere, that is immersed in water,
- Steel liner that is structurally backed by reinforced concrete is not structurally challenged.

Moreover, it is important to note that a splinter scenario exists for creep failure of the main steam line due to it being heated up to ~1,000 K, a situation that would appear quite credible, even based on the rough predictions of upper plenum temperatures, and that would yield natural depressurization, and avoidance of melt ejection altogether. Interestingly, the so-made transition to low pressure would make available the GDCS for safety injection, thus possibly arresting the meltdown process.

19.3.3.6 References for DCH

19.3.3-1 T.G. Theofanous (1996), “On the Proper Formulation of Safety Goals and Assessment of Safety Margins for Rare and High-Consequence Hazards,” Reliability Engineering & Systems Safety, 54 (1996) 243–257.

19.3.3-2 J.H. Scobel, T.G. Theofanous and S.W. Sorrell, “Application of the Risk Oriented Accident Analysis Methodology (ROAAM) to Severe Accident Management in the AP600 Advanced Light Water Reactor,” Reliability Engineering and Safety Systems, 62 (1998) 51-58.

19.3.3-3 M.M. Pilch (1994), Continued Enlargement of the Initial failure Site in the Reactor Pressure Vessel. Appendix J in NUREG/CR-6075, SAND93-1535. Also, Nuclear Engineering and Design, 164 (1996).

19.3.3-4 M.M. Pilch, H. Yan and T.G. Theofanous (1996), “The Probability of Containment Failure by Direct Containment Heating in Zion,” Nuclear Engineering & Design, 164 (1996) 1–36.

19.3.3-5 M.M. Pilch and Allen, M. D. (1996) "Closure of the direct containment heating issue for Zion”, Nuclear Engineering & Design, 164, pp.37-60.

19.3.3-6 M.M. Pilch, (1996) "A Two-Cell Equilibrium Model for Predicting Direct Containment Heating", Nuclear Engineering & Design, 164, pp.61-94.

19.3.3-7 H. Yan and T.G. Theofanous, "The Prediction of Direct Containment Heating," Nuclear Engineering & Design, 164 (1996) 95–116.

19.3.3-8 G.P. Reddy and D.J. Ayers (1982), "High-Temperature Elastic-Plastic and Creep Properties for SA533 Grade B Class I and SA508 Materials", EPRI NP-2763, Electric Power Research Institute.

19.3.3-9 G.V. Smith (1971), "Evaluation of the Elevated Temperature Tensile and Creep Rupture Properties of C-Mo, Mn-Mo, and Mn-Mo-Ni Steels", Metal Properties Council, American Society for Testing and Materials, ASTME Data Series Publication DS47.

19.3.3-10 NEDC-33201 GE's ESBWR Certification PRA Report, (2005)

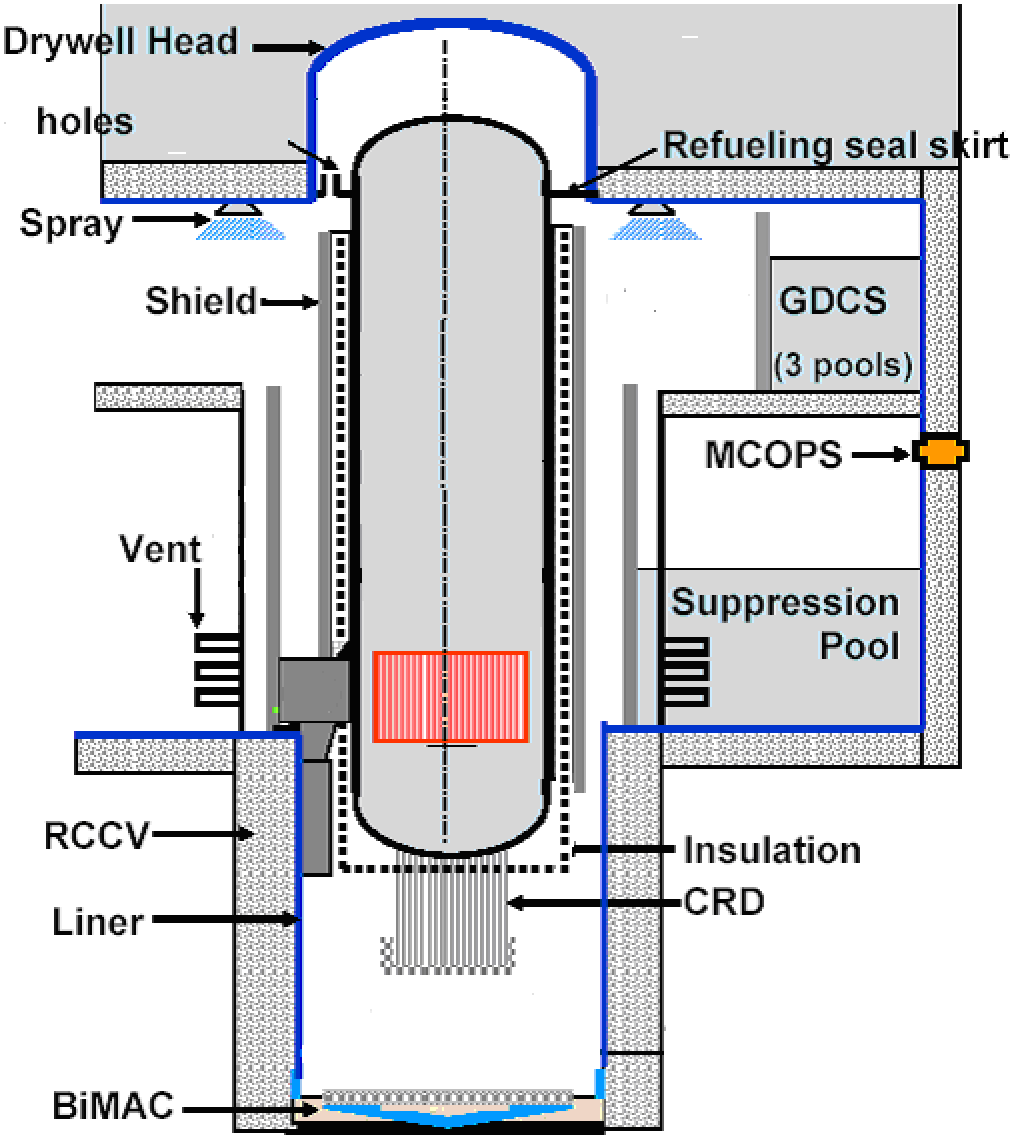


Figure 19.3.3-1. Illustration of the ESBWR Drywell for Severe Accident Phenomena

Note: Dimensions and arrangement of important volumes of LDW, UDW and annular airspaces connecting LDW to UDW, and vents to suppression pools are provided to scale. The annular space between the shield and the RPV is filled with insulation materials. The spray provides cooling to the drywell atmosphere after the DCH event.

19.3.4 Ex-Vessel Steam Explosions (EVE)

19.3.4.1 Overall considerations

Ex-Vessel Steam Explosions (SE) are energetic fuel-coolant interactions that are triggered from already premixed states developed as the melt released from the RPV falls into, and traverses the depth of a water pool below. Metallic melts such as those expected here for low pressure scenarios are especially prone to such energetic behavior. The result is pressure pulses that may reach the magnitude kbar range. They are not quite sufficient to generate self-sharpening shock waves in water, but are potentially capable, when large quantities of melt are involved together with highly subcooled water, of loading major structures to failure. Failure is characterized by the impulse—the time-integral of the pressure acting on the surface of the structure.

While in-vessel explosions (IVE) are essentially of exclusive interest to PWRs, ex-vessel explosions (EVE) are of primary interest to BWRs. One reason is that in BWRs the initial release is mostly metallic. Another reason is that LDW designs have traditionally employed very large-height geometries, which, when flooded, form deep water pools below the reactor vessel.

From another perspective, these large geometries in BWRs have been thought of as a means to assuring long-term coolability for a core-on-the-floor scenario. The idea in this case is that deep flooding would provide sufficient travel distance for the melt to fragment and quench, thus forming a coolable debris bed on the LDW floor.

Our approach in ESBWR is to minimize the likelihood of deep subcooled water pools in the LDW at the time of vessel failure, and to have a structural design capable of coping with the loads expected in cases where moderate amounts of water (shallow, saturated pools) cannot be avoided. This “coping” in the presence of shallow, saturated pools is based on:

a. The simple idea of explosion venting (Theofanous and Yuen, 1995) — an effect that produces a smaller impulse by reducing both the time for the pressure wave unloading at the pool surface, as well as the amplitude of the wave that propagates radially outwards and,

b. The known behavior that premixtures in saturated water pools are highly voided, thus becoming resistant to triggering and supporting detonation waves, and moreover, even if possible, explosions would be highly inefficient (Henry and Fauske, 1981; Theofanous et al., 1987).

19.3.4.2 ESBWR Design

Regarding the potential damage from EVE, the relevant structures are the reactor pedestal reinforced concrete wall as illustrated in Figure 19.3.4-1, and the BiMAC device, a layer of thick-walled steel pipes that are well embedded into reinforced concrete that supports them in all directions as shown in Figure 19.3.4-2. The structural details of both are described in the NEDC-33201 report. Failure of the reactor pedestal, along with the steel liner on it, would constitute violation of the containment boundary. While at static condition the load-bearing capacity of this structure is adequate, explosive-level pressures acting on millisecond time scales can produce sufficient extent of concrete cracking, along with liner stretching and tearing, to compromise leak-tightness of the containment. Failure of the BiMAC device on the other hand is defined as crushing of the pipes so that they cannot perform their heat removal function —

channeling the so-generated two-phase mixture from the bottom onto the top of the debris mass. Such failure would raise the possibility of continuing corium-concrete interactions, basemat penetration, and containment pressurization by the so-generated non-condensable gases.

The principal element of our severe accident management approach on EVE is to address the quantities (subcooling) of water in the LDW, just prior to melt exiting the RPV. It is at this time that the relocation can be potentially massive, and thus of energetic concern. The situation can be summarized as follows:

a. As a result of early interactions of this effort with Level-1 PRA and the designers, modifications in the containment design were made to prevent subcooled water, to the extent possible, from entering the LDW through the UDW; in particular this covered the re-routing of GDCS overflow, and outfitting the WW spill-over lines with squib valves, similarly to those that activate the equalizer line.

b. A BiMAC device activation system requires high temperature thermocouples, located under the LDW basemat, to detect core-melt arrival and send signals to actuate opening of the LDW deluge lines (feeding off the GDCS pools) so that premature flooding is to be reliably prevented.

Item (b), as discussed in the NEDC-33201 report, is based on a BiMAC design that makes it function immediately upon opening the deluge lines. Thus there is no need to pre-flood the LDW, and deluge lines valve activation system detailed design is based upon detecting melt arrival onto the LDW floor. This activation system is accessible both automatically as well as by operator action, and the required reliability is such that the failure frequency is less than 10^{-3} failure per demand.

19.3.4.3 Previous Work

The Steam Explosions Review Group (SERG) convened by the US NRC, focused on the alpha mode containment failure (SERG-1, 1985; SERG-2, 1995). Thus only in-vessel steam explosions for PWRs were considered in detail. For BWRs, the lower plenum design, largely and densely occupied by control rod guide tubes, was considered to be generically prohibitive of the large scale events required for α-failure. Other licensing-related work for in-vessel steam explosions is the ROAAM-based consideration of lower head integrity for the AP600 (Theofanous et al, 1999c).

Major milestones in the understanding the physics of steam explosions and in the development of computational and modeling technology for simulating energetics have been summarized in NEDC-33201 and steam explosion references sited in the same report. The key idea in modeling energetics is that of “microinteractions” (Yuen and Theofanous, 1999). The computer codes PM-ALPHA (Yuen and Theofanous, 1995) and ESPROSE.m (Yuen and Theofanous, 1995), for premixing and propagation respectively, are still the state-of-the-art (CFD simulation) tools. Verification and validation of these codes has been documented and reviewed extensively (full ROAAM review) during the AP600 Design Certification effort. These codes now are also used by the US NRC consultants during licensing reviews such as for ex-vessel explosions in the AP1000

There is no previous work on fragility to impulsive loads of a structure such as the BiMAC. Previous assessments of thick reinforced concrete walls, done only in a very crude manner

(Rashid, Theofanous, and Foadian, 1995) , indicates that an impulse magnitude of ~100 kPa.s could begin to inflict significant damage (cracking) on a reinforced concrete wall (pedestal) that is 1.5 m thick. At such levels of explosion impulse, cracking was found to be significantly reduced for a 7,000 psi concrete, and to be virtually eliminated for a 10,000 psi concrete. However, such improved grades of concrete are more expensive than the "normal", 5,000 psi grade considered for ESBWR.

19.3.4.4 Present Assessment

19.3.4.4.1 Key Physics

In an open system, such as the LDW of the ESBWR, the susceptibility of a pre-mixture to triggering decreases as the volume fraction of steam (the void fraction) in it increases; thus subcooled water pools are considerably more prone to energetic behavior in comparison to saturated pools. On the other hand, the energetics of an explosion increases along with the total quantity of melt found in the pre-mixture at the time of triggering; thus explosions in deep pools can be more damaging in comparison to those in shallow pools. Both of these features, the subcooling and the depth, couple with a host of other parameters (melt mass break-up, momentum exchanges between all melt and coolant, phase changes of coolant, etc) in a highly dynamic set of phenomena, to produce, for any particular mixing realization, an evolution of pre-mixtures, each one with a particular susceptibility to triggering and efficiency in thermal-to-mechanical energy conversion. As in the previous assessments done for licensing purposes (Theofanous et al, 1999c), both triggering and efficiency are treated here in a bounding fashion; that is, triggering is assumed to occur at the time of most favorable (least voided) premixture, and key limitations to energetics, such as fuel freezing during premixing, and non-equilibrium in the micro-interactions are not accounted for. In assessing EVE loads, we rely on well-qualified mechanisms and tools to account for pressure wave unloading/venting phenomena, applied to idealized/efficient explosions.

Current understanding of structural integrity under impulsive loading derives from work with high explosives (HE), acting mostly within a gaseous medium. In comparison to these explosions, in EVEs the pressure pulses would be of much lower amplitudes and of a much longer duration. Still, with a structure whose natural frequency is much longer than the pulse width, it is the delivered impulse that characterizes damage, and existing HE-derived tools, such as the LS-DYNA3D code used in this work (Noble et al, 2005), can be expected to be well applicable. Again conservatively, in this application, we ignore the dissipative effects (and so-reduced actual loading) due to fluid-structure interaction. That is, pressure pulses obtain from explosion calculations based on rigid wall geometry, are then applied to the structural calculation.

As concrete is highly resistant to compression but rather weak in tension, the mode of failure for the reactor pedestal is concrete cracking, separation from the rebar net, spallation at the "free end", and wall-yielding that result in displacements sufficient to strain the liner to failure. To lose containment integrity, either the liner must be strained to failure (typically ~30% effective plastic strain), or the wall must be damaged enough to not be able to stand under the dead weight. The reinforcement, sometimes pre-tensioned, is employed to balance load-bearing performance in this respect. However, at the kbar range of pressures of interest here, this load bearing is to reduce the extent, rather then eliminate cracking, and in any case it is not considered in this assessment. For the BiMAC, the same mechanisms are superposed to yield deformation of the steel pipes, and eventual plastic yielding to produce collapse, and thus failure of BiMAC function.

19.3.4.5 Summary and Conclusions for EVE

The detailed probabilistic framework, quantification of EVE loads, quantification of fragility to EVE, and prediction of failure probability due to EVE are described in the GE PRA report NEDC-33201. The results on EVE described in NEDC-33201 show that for all but less than 1% of the CDF, involving deep and subcooled water pools, violation of the ESBWR containment leak-tightness, and of the BiMAC function, due to ex-vessel explosions are physically unreasonable.

Principal ingredients to such a conclusion can be recapitulated as follows:

(1) An accident management strategy, and related hardware features that prohibit large amounts of cold water from entering the LDW prior to RPV breach,

(2) The physical fact that premixtures in saturated water pools become highly voided and thus unable to support the escalation of natural triggers to thermal detonations,

(3) Reactor pedestal and BiMAC structural designs that are capable to resist explosion load impulses of magnitudes in the 100's of kPa.s.

19.3.4.6 References for EVE

19.3.4-1 T.G. Theofanous and W.W. Yuen, "The Probability of Alpha-Mode Containment Failure Updated," Nuclear Engineering & Design 155 (1995) 459–473.

19.3.4-2 R.E. Henry and H.K. Fauske (1981), "Required Initial Conditions for Energetic Steam Explosion", ASME HTD v.19, pp.99-108.

19.3.4-3 T.G. Theofanous, B. Najafi and E. Rumble (1987), "An Assessment of Steam-Explosion-Induced Containment Failure. Part I: Probabilistic Aspects," Nuclear Science and Engineering, 97, 259-281 (1987). M.A. Abolfadl and T.G. Theofanous, "An Assessment of Steam-Explosion-Induced Containment Failure. Part II: Premixing Limits," Nuclear Science and Engineering, 97, 282-295 (1987). W. H. Amarasooriya and T.G. Theofanous, "An Assessment of Steam-Explosion-Induced Containment Failure. Part III: Expansion and Energy Partition," Nuclear Science and Engineering, 97, 296-315 (1987). G.E. Lucas, W.H. Amarasooriya and T.G. Theofanous, "An Assessment of Steam-Explosion-Induced Containment Failure. Part IV: Impact Mechanics, Dissipation and Vessel Head Failure," Nuclear Science and Engineering, 97, 316-326 (1987).

19.3.4-4 NEDC-33201, GE PRA Report for ESBWR, (2005).

19.3.4-5 SERG (1985) Review of the current understanding of the potential for containment failure from in-vessel steam explosions, NUREG-1116, U.S. NRC (1985).

19.3.4-6 SERG-2 (1995) Proceedings of the Second Steam Explosion Review Group (SERG-2) Workshop, NUREG-1524, ed., S. Basu and T. Ginsberg, August 1996. (Follow-on international FCI research summarized in Proceedings of the OECD/CSNI Specialists

Meeting on Fuel-Coolant Interactions, NEA/CSNI/R(97)26, ed., M. Akiyama, N. Yamano and J. Sugimoto, January 1998.)

19.3.4-7 T.G. Theofanous, W.W. Yuen and S. Angelini (1999a), "The Verification Basis of the PM-ALPHA Code," Nuclear Engineering & Design, 189 (1999) 59-102. (Also T.G. Theofanous, W.W. Yuen and S. Angelini, "Premixing of Steam Explosions: PM-ALPHA Verification Studies," DOE/ID-10504, June 1998.). T.G. Theofanous, W.W. Yuen, K. Freeman and X. Chen (1999b), "The Verification Basis of the ESPROSE.m Code," Nuclear Engineering & Design, 189 (1999) 103-138. (Also T.G. Theofanous, W.W. Yuen, K. Freeman and X. Chen, "Propagation of Steam Explosions: ESPROSE.m Verification Studies," DOE/ID-10503, June 1998.).

19.3.4-8 W.W. Yuen and T.G. Theofanous, "PM-ALPHA: A Computer Code for Addressing the Escalation/Propagation of Steam Explosions," DOE/ID-10501, April 1995.

19.3.4-9 W.W. Yuen and T.G. Theofanous, "On the Existence of Multiphase Thermal Detonations," Int. Jl. Multiphase Flow, 25 (1999) 1505-1519.

19.3.4-10 W.W. Yuen and T.G. Theofanous, "PM-ALPHA: A Computer Code for Addressing the Premixing of Steam Explosions," DOE-10502, May 1995.

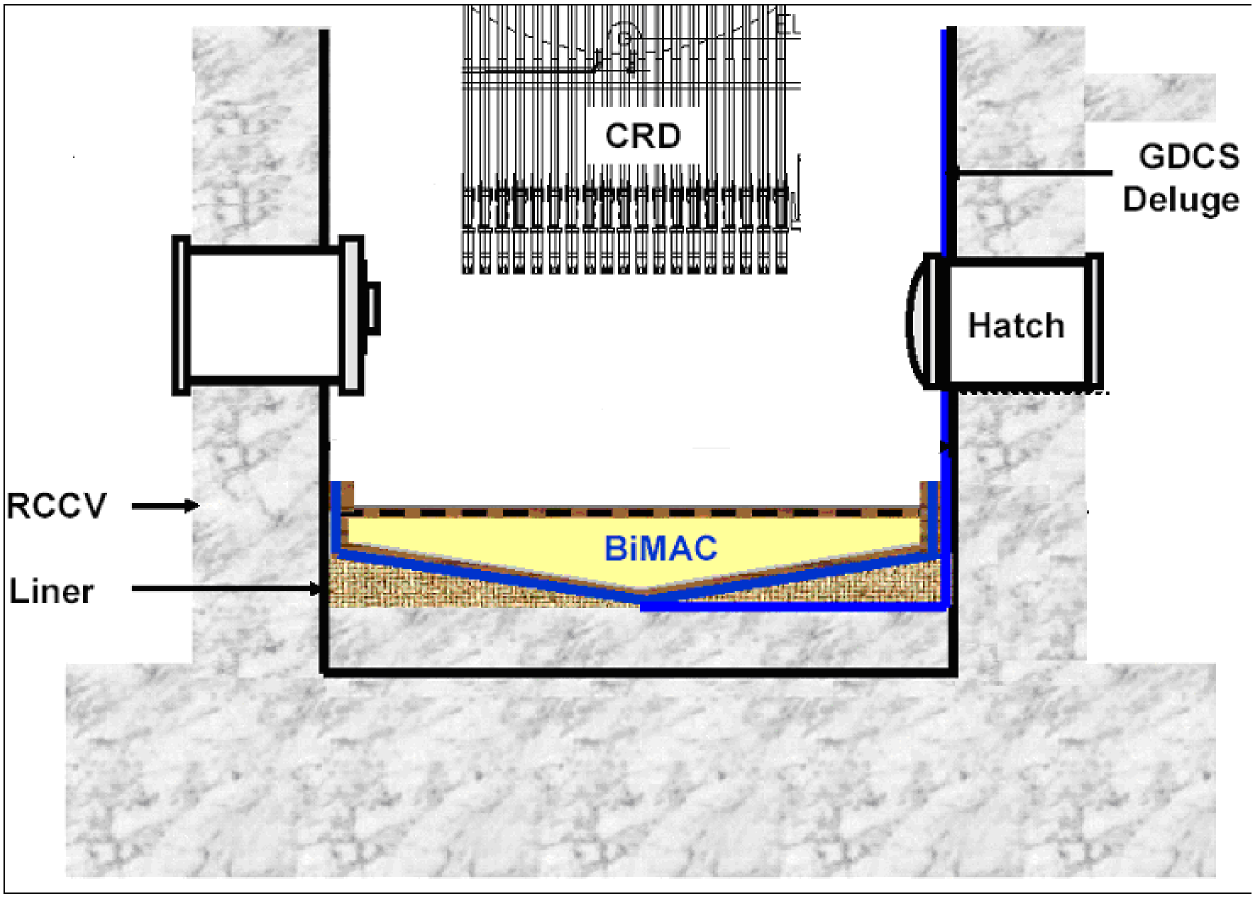


Figure 19.3.4-1. Containment Structural Composition and Boundary in the LDW Region

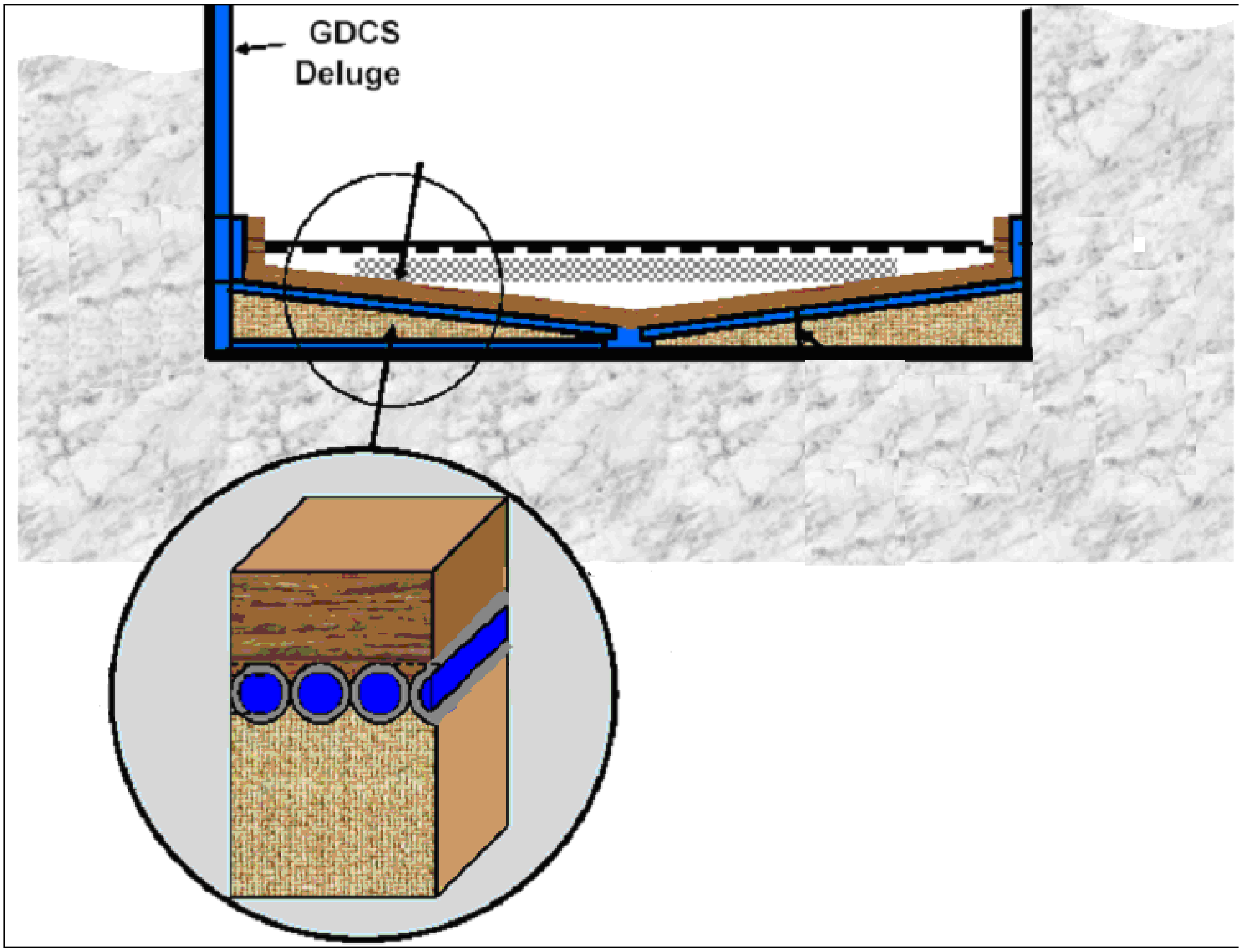


Figure 19.3.4-2. BiMAC Device in the Pedestal Region

19.3.5 Basemat Melt Penetration (BMP)

19.3.5.1 Overall Considerations

For all currently operated LWRs, the severe accident management case is based on the so-called core-on-the-floor concept. The basic premise is that, provided there is sufficient floor area available for spreading and sufficient amount of water to cover the molten core debris, the debris will become quenched, and will remain coolable thereafter. While work appears to be continuing, operation of reactors is justified on the basis of analyses that are claimed to satisfy the so-called 24-hour rule. These analyses assume a split of decay power between the upwards (into water) and downwards (into concrete) directions, and predict that (a) basemat penetration will not occur for a minimum of 24 hours, and (b) containment will not fail by accumulation of so-generated non-condensable gases also for a minimum of 24 hours.

While ESBWR satisfies the basic conditions for this approach, that is the core-melt spreadable floor area according to the EPRI URD guidelines for advanced reactors, and while analyses such as those described above show that the 24-hour rule is satisfied with great margins (more than 72 hours), this core-on-the-floor approach is further improved. We have incorporated in the design features that make the issue of corium-concrete interactions, along with the great uncertainties that arise in its consideration, mute.

The importance of assuring long term coolability has been also appreciated by the designers of all advanced passive plants of the future: the AP600 is provided with features that assure in-vessel retention and coolability, the AP1000 has followed the same approach, and the European Pressurized Reactor (EPR) design placed this line of defense ex-vessel, by means of a rather elaborate scheme for facilitating corium spreading and heat removal (Fisher, 2003). The new Russian V-320 design of VVER1000 plant (under construction in Tianwan, China) has a very elaborate ex-vessel core catcher, which includes a basket made of Al_2O_3-Fe_2O_3-steel mixture and filled with a special material compound (Kukhtevich, 2001).

19.3.5.2 ESBWR Design

ESBWR design uses a passively-cooled boundary that is impenetrable by the core debris in whatever configuration it could possibly exist on the LDW floor. For ex-vessel implementation, this boundary is conveniently, and advantageously made by a series of side-by-side placed inclined pipes, forming a jacket which can be effectively and passively cooled by natural circulation when subjected to thermal loading on any portion(s) of it. Water is supplied to this device from the GDCS pools via a set of squib-valve-activated deluge lines. The timing and flows are such that (a) cooling becomes available immediately upon actuation, and (b) the chance of flooding the LDW prematurely, to the extent that opens up a vulnerability to steam explosions, is very remote. The jacket is buried inside the concrete basemat and would be called into action only in the event that some or all of the core debris on top is non-coolable.

The device, called Basemat Internal Melt Arrest and Coolability device (BiMAC) is illustrated in Figure 19.3.5-1. Important considerations in implementation of this concept are as follows:

> **Pipe inclination angle.** As we show further below, both the thermal load due to melt natural circulation (q_D), and the burnout critical heat flux (the CHF), increase with angle of inclination of the bottom boundary from the very low values pertinent for a perfectly

horizontal orientation. This increase is much faster for the CHF in the region $0<\theta<20^0$, and there is a maximum separation from q_D at around the upper end of this range. Within a reasonable value of the overall vertical dimension of the BiMAC device, the whole LDW can be covered conveniently with pipes inclined at near the upper end of this range.

Sacrificial refractory layer. A refractory material is laid on top of the BiMAC pipes so as to protect against melt impingement during the initial (main) relocation event, and to allow some adequately short time for diagnosing that conditions are appropriate for flooding. This is to minimize the chance of inadvertent, early flooding. The material is selected to have high structural integrity, and high resistance to melting such as ceramic Zirconia.

Cover plate. As shown in Figure 19.3.5-1, we use a supported steel plate to cover the BiMAC. On the one hand this allows that the top is a normal floor as needed for operations, and that the BiMAC is basically "out of the way" until its function is ever needed. On the other hand the so-created cavity, with a total capacity of ~100 m^3, is there to receive and trap the melt in a hypothetical ex-vessel severe accident evolution, including a high pressure melt ejection. For this purpose the top plate is stainless steel of thickness such as to be essentially instantaneously penetrable by a high-velocity melt jet. The plate is made to sit on top of normal floor grating, which itself is supported by steel columns as indicated schematically in Figure 19.3.5-1. Further details on this simple support system are straightforward engineering tasks pertinent to the COL stage of the plant design and review. Between the plate and the grating we have a layer of refractory material, like a mat of zirconium oxide, so as to protect the steel material from thermal loads from during the ~ 40 seconds steam blow-down period, yet not able to provide any structural resistance to melt penetration as needed for the trapping function noted above. For low pressure sequences, this whole cover structure has no bearing on the outcome.

The BiMAC cavity. The space available below the BiMAC plate is sufficient to accommodate the full-core debris, and the entire coolable volume, up to the height of the vertical segments of the BiMAC pipes is ~400% of the full-core debris. Thus there is no possibility for the melt to contact the LDW liner. Similarly, the two sumps needed for detecting leakage flow during normal operation, are positioned and protected, as is the rest of the LDW liner, from being subject to melt attack.

The LDW deluge system. According to the preliminary design, this system consists of three main lines that feed off the three independent GDCS pools, respectively, each separating into a pair of lines that connect to the BiMAC main header (see Figure 19.3.5-1). As noted above, the required failure rate of the system does not exceed 10^{-3} per failure per demand.

19.3.5.3 Previous Work

The IVR coolability work was done under DOE's ARSAP program. This IVR technology includes the initial (Configuration I) ULPU tests that quantify CHF as a function of inclination (Theofanous and Syri, 1997), the ACOPO tests that quantify natural convection loads from volumetrically-heated pools (Theofanous and Angelini, 2000), and ROAAM that provides the organizing principle for the whole assessment (Theofanous et al, 1994, 1996). One major simplification at present is that the behavior is not susceptible to the so-called "focusing effect", a phenomenon that can arise in in-vessel situations when there is an insufficient amount of molten steel to spread the heat over a large enough area of the side wall, together with the absence of water on top of the molten pool.

Since this early work, there has been an intense follow-up internationally on IVR, including a CSNI specialist's meeting (Garching, 1994), several test programs in France (SULTAN tests), Finland (COPO tests, VTT tests), Sweden (SIMECO, FOREVER tests), Korea (KAIST tests), and Russia (RASPLAV, MASCA).

In addition, and on fundamental grounds, since that time the mechanism of Boiling Crisis is understood better (Theofanous et al., 2002a, 2002b; Theofanous and Dinh, 2002, 2004). So is natural convection (Theofanous and Angelini, 2000; Dinh et al., 2004a, 2004b), which has been also greatly impacted by advances in CFD and computing power that allow rather detailed Direct Numerical Simulations (DNS) of such phenomena with great reliability. Use is made of this simulation capability for assessing the thermal loads in the present 2D-conical (or wedge-) shaped geometry.

19.3.5.4 Present Assessment

Key Physics

Successful functioning of the BiMAC devise depends crucially on the condition that heat removal capability by boiling exceeds the thermal loading due to melt natural convection. The key physics are the processes that control the magnitude of these two outcomes. In addition, it must be shown that, at the end of the main melt relocation event, and associated ablation process, the BiMAC sacrificial layer is left with some material still protecting the steel pipes.

a. **Thermal Loads**. Any amount of core debris that is not coolable, will form into a molten pool that, heated in volume, and rejecting heat to the outside through all its boundaries, would eventually reach a quasi-steady, maximum extend configuration. This means that such a molten pool would tend to spread, incorporating more and more debris and concrete material, until eventually all heat supplied to all of its boundaries from within is removed by conduction through the surrounding solid crusts and associated materials found without. Thus at the top boundary, it being in contact with water, this balance between heat supply and rejection would define the thickness of the solidified material assumed to exist, persist, and be impenetrable to water; for otherwise, the debris would be coolable on its own, without a need for BiMAC. At the bottom boundary, the melting would extend eventually to a degree that only a rather thin layer of remaining sacrificial material and solidified debris would separate the melt from the steel pipes below. Thus, all around the inside the molten pool would see the liquidus temperature, while it develops the amount of superheat needed for rejecting the decay power generated within. We are primarily interested in the thermal loads delivered to the lower, wedge-shaped boundary, and to any vertical boundaries for pools voluminous enough to create submergence of the vertical pipe segments. Bounding estimates of these loads are obtained by assuming a maximum extent pool consisting of the total amount of core-and-internals debris possible. From previous experience (for example Angelini and Theofanous, 1995) with this type of large, high Rayleigh number pools, we know these loads are spatially non-uniform and the magnitudes increase with angle of inclination of the lower boundary, reaching a maximum at vertical boundaries.

b. **Limits of Coolability**. These limits are defined by the burnout heat flux, or Critical Heat Flux (CHF), of water boiling on the inside of the inclined BiMAC pipes. Previous experience in such geometries (Theofanous and Syri, 1997) shows that the CHF increases rapidly with angle of inclination, and that this increase is most rapid in the 0 to 20 degrees interval ranging from 300 kW/m2 at the low end to 500 kW/m2 at the upper end. More recent fundamental data show that burnout in nucleate boiling occurs due to dryout of extremely thin liquid films (tens of microns in thickness) and that surface wettability plays a key role in this dryout (Theofanous et al, 2002a-b). Engineering surfaces such as those of the steel pipes employed here were found to be very resilient to dryout. Still, assessment of CHF for any new situation is a matter for empirical determination under the appropriate geometry and fluid flow conditions representative of the application. This was in particular the case for the AP600 and AP1000 (Theofanous et al, 1996, and Dinh et al, 2003), and is the approach we take here.

c. **Sacrificial Material Ablation by Jet Impingement**. Heat transfer and related phase change processes during melt jet impingement on a solid slab were studied in the past and their mechanisms are well understood (Theofanous et al., 1996). Notably, due to the high melting point of the jet's liquid, compared to the slab's initial temperature, a crust is formed and serves as thermal boundary condition, through which the heat transfer occurs. In other words, the melt superheat (relative to melt liquidus), along with the jet velocity, is the main driving force for the impingement heat transfer under phase changes. If the slab material's melting point is lower than the jet's crust temperature, the slab is ablated and its material is swept away by the melt flow. In BiMAC, we use a refractory material with high melting point temperature on the interior cover, thus eliminating the threat of superheated, metallic melt jets. As opposed to being ablated and swept away by the jet flow, the refractory layer remains structurally intact and limits the heat transfer by conduction in a low-conductivity medium.

19.3.5.5 Summary and Conclusions for BMP

The detailed probabilistic framework, quantification of BMP loads, quantification of fragility to BMP, and prediction of failure probability due to BMP are described in the GE PRA report NEDC-33201. The result of BMP device analysis described in NEDC-33201 show that the BiMAC device is effective in containing all core melts in a manner that assures long term coolability and stabilization of the resulting debris. In this way the concrete basemat penetration issue becomes moot, as is containment over-pressurization by the so-generated concrete decomposition gases

The principal ingredients in this effective functioning of the device can be summarized as follows:

(1) Choice a refractory ceramic, that eliminates ablation by superheated metallic jets, which are the most aggressive, and the thickness is chosen to provide ample margins to ablation by large-volume, superheated oxidic jets (both for LP and HP scenarios),

(2) Positioning and dimensioning of the cooling jacket (the BiMAC pipes) so that while resistant to significant dynamic loads (see Section 19.3.4), they allow for stable, low-loss, natural circulation that is not susceptible to dryouts,

(3) Positioning the BiMAC in the LDW in such a way that all melt released from the vessel is captured (except any melt dispersed to the UDW in HP scenarios) and contained within it, and

(4) Providing for an angle of inclination of the lower boundary that balances the various requirements, including operational space available, and good margins to local burnout.

Full-scale testing of BiMAC is straightforward, and needed for final confirmation and optimization of the design at the COL stage.

19.3.5.6 References for BMP

19.3.5-1 M. Fischer, (2003). “Severe Accident Mitigation and Core Melt Retention in the European Pressurized Reactor (EPR)”, *11th International Conference on Nuclear Engineering*, Tokyo, JAPAN, April 20-23, 2003, ICONE11-36196.

19.3.5-2 I.V. Kukhtevich, V.V Bezlepkin and Yu. G. Leontiev , V. Strizhov , V.B. Proklov, (2001). “Severe Accident Management Measures for Tianwan NPP with VVER-1000, in “Implementation of Severe Accident Management Measures”, Workshop Proceedings PSI-Villigen, Switzerland, 10-13 September 2001. Nuclear Safety NEA/CSNI/R, (2001)

19.3.5-3 T.G. Theofanous and S. Syri, (1997). “The Coolability Limits of a Reactor Pressure Vessel Lower Head,” Nuclear Engineering & Design, 169, 59–76, 1997.

19.3.5-4 T. G. Theofanous, and S. Angelini, (2000). “Natural Convection for In-Vessel Retention at Prototypic Rayleigh Numbers,” Nuclear Engineering and Design, 200, 1-9, 2000; T.G. Theofanous, C. Liu, S. Angelini, O. Kymäläinen, H. Tuomisto and S. Additon, (1994a). “Experience From the First Two Integrated Approaches to In-Vessel Retention Through External Cooling,” OECD/CSNI/NEA Workshop on Large Molten Pool Heat Transfer, Nuclear Research Centre, Grenoble, France, March, 9–11, 1994.; T.G. Theofanous, S. Syri, T. Salmassi, O. Kymäläinen and H. Tuomisto, (1994b). “Critical Heat Flux Through Curved, Downward Facing, Thick Walls,” Nuclear Engineering & Design, 151, 247-258, 1994; T.G. Theofanous, S. Syri, T. Salmassi, O. Kymäläinen and H. Tuomisto, (1994c). “Critical Heat Flux Through Curved, Downward Facing, Thick Walls,” OECD/CSNI/NEA Workshop on Large Molten Pool Heat Transfer, Nuclear Research Centre, Grenoble, France, March, 9–11, 1994.

19.3.5-5 T.N. Dinh, J.P. Tu and T.G. Theofanous, “Hydrodynamic and Physico-Chemical Nature of Burnout in Pool Boiling”, International Conference on Multiphase Flow, Yokohama, Japan, May 2004. Paper 296. 14p.

19.3.5-6 Garching (1998) OECD/CSNI/NEA Workshop on “In-vessel core debris retention and coolability”, Garching, Germany, 3-6 March, 1998.

19.3.5-7 T.G. Theofanous, J.P. Tu, A.T. Dinh and T.N. Dinh, (2002a). "The Boiling Crisis Phenomenon. Part I: Nucleation and Nucleate Boiling Heat Transfer", Experimental Thermal and Fluid Science, 26, 775-792, 2002.

19.3.5-8 T.G. Theofanous, J.P. Tu, A.T. Dinh and T.N. Dinh, (2002b). "The Boiling Crisis Phenomenon. Part II: Dryout Dynamics and Burnout", *Experimental Thermal and Fluid Science* 26, 793-810, 2002.

19.3.5-9 T.G. Theofanous, and T.N. Dinh (2004), "High Heat Flux Boiling and Burnout as Microphysical Phenomena: Mounting Evidence and Opportunities", accepted for *Multiphase Science and Technology*. 2005. Also *Keynote Paper*. Japan-US Seminar on Two-Phase Flow Dynamics. December 6-11, 2004. Nagahama. CD-ROM Proceedings.

19.3.5-10 T.N. Dinh, Y.Z. Yang, J.P. Tu, R.R. Nourgaliev and T.G. Theofanous (2004a), "Rayleigh-Bernard Natural Convection Heat Transfer: Pattern Formation, Complexity and Predictability", *2004 International Congress on Advances in Nuclear Power Plants*, Pittsburgh, PA, June 13-17, 2004. Also, T.N. Dinh, J.P. Tu, Y.Z. Yang, R.R. Nourgaliev and T.G. Theofanous (2004b), "Characterization and Predictability of Transient Heat Transfer in an Unstably Stratified Layer during Power Startup", *37th AIAA Thermophysics Conference*, Portland, OR, June 27-30, 2004. AIAA-2004-2733.

19.3.5-11 NEDO-33201 GE's ESBWR Certification PRA Report, (2005)

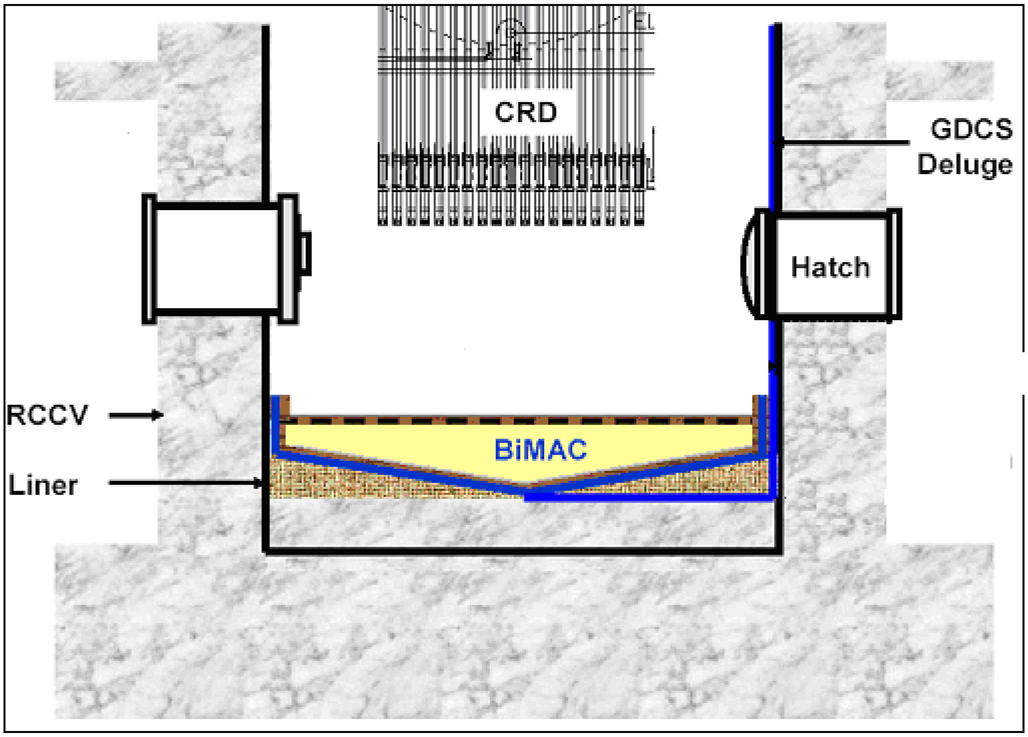


Figure 19.3.5-1. BiMAC in the LDW

The BiMAC in the LDW. The initial flooding and cooling is provided by flow from Gravity-Driven Cooling System (GDCS) deluge.

19.3.6 Results and Conclusions

The purpose of this section is to summarize the results of the previous sections in a form that is suitable for use in the Level-2 and Level-3 PRA of ESBWR.

In ROAAM we acknowledge that when the basis of evaluation is epistemic, probabilities are subjective, and quantification of such probabilities cannot be done, in substance, any other way but in terms of definitions that themselves are of subjective/epistemic character. Thus a numerical probability scale is used only for the purpose of propagating uncertainty, and we insist that the end results be only interpreted in terms of the same probability scale (see Table 19.3.6-1) applied in reverse.

This kind of procedure was used in all previous applications of ROAAM (as enumerated in Section 19.3.2), and for purposes of issue resolution such a finely qualitative interpretation of the results seemed to be appropriate and sufficient. In the present case the situation is different in two ways: (a) for all potential containment threats, strongly bounding arguments could be made at a level of generality, and margins that obviated the need for propagation of uncertainty, and (b) a final reinterpretation in quantitative terms suitable for PRA use is, in fact, a requirement for licensing reviews. The implication of item (a) is that according to the ROAAM "quality of evaluation" criteria (see Table 19.3.6-.2); this assessment is at most desirable, high-confidence level, or Grade A. The consequence of item (b) is that we still need to convert, such high confidence (essentially deterministic) results, to probability estimates.

More specifically, because we have found that all containment threats (in postulated ESBWR severe accidents that were not assigned to the "residual risk" category) are "physically unreasonable", our task is to simply interpret this level of likelihood. Opinions on this can differ, so, to simplify matters, we will take the approach that this level of probability will have to be something greater than 0.1%.

Table 19.3.6-1

Definition of Probability Levels

Process Likelihood	Process Characteristic
1/10	Behavior is within known trends but obtainable only at the **edge-of-spectrum** parameters
1/100	Behavior cannot be positively excluded, but it is **out side the spectrum** of reason
1/1000	Behavior is **physically unreasonable** and violates well-known reality. It occurrence can be argued against positively

Table 19.3.6-2

Definition of Quality Grades

Grade A	Framework characterized by **a simple, limiting process**, evaluated on basic physical laws, with appropriate bounding inputs. **No scenario dependence**.
Grade B	Framework involves **a single complex process** evaluated at a high confidence level. There may be **slight scenario dependence** compensated by appropriate quantification of intangibles.
Grade C	Framework involves **sequence of processes**. Significant scenario dependence compensated by appropriate choice of intangibles and splinter scenarios.

19.4 PRA INSIGHTS AFFECTING ESBWR DESIGN

19.4.1 Introduction

The ESBWR PRA was developed in parallel with the ESBWR design. As a consequence the design has benefited from the preliminary results of the PRA, which influenced the selection of design alternatives that resulted in a maximum reduction of risk.

In this section, the results of the PRA are reviewed to highlight the important ESBWR design characteristics that have been shown relevant in the various PRA analyses and contributed more significantly to the mitigation or prevention of a particular accident sequence or event scenario.

19.4.2 Insights from Level 1 Internal Events Analysis

The specific design features identified below provided an important contribution to safety in the level 1 internal events analysis:

(1) Isolation Condenser System (ICS)

The ICS is able to maintain reactor pressure and temperature within an acceptable range so that Safety/Relief valves will not lift following pressurization events. This minimizes the chance that a relief valve will stick open and eventually defeat the ICS system performance. The system also maintains reactor vessel inventory so that reactor automatic depressurization will not occur when the reactor becomes isolated. The IC/PCC pools, in conjunction with the refueling pool, provide enough water inventory for decay heat removal beyond 72 hours. The system redundancy, independence and diversity of actuation signals contribute significantly to lowering the risk of isolation transients.

Another important feature of ICS is that it can perform its function for the first 24 hours without any electric power (AC or DC) whatsoever. This combined with fire water makeup to the ICC pool provides a robust mitigating system for isolation transients.

(2) Control Rod Drive High Pressure Makeup (HPCRD)

The HPCRD system is able to provide RPV makeup when the reactor is at high pressure. The flow rate is high enough that it can provide cooling to balance decay heat shortly following a reactor scram. It is automatically initiated when water level drops below Level 2. This allows the RPV level to be recovered for nearly all events. This active system provides an active backup to ICS for transient conditions. The redundancy and diversity in the system design contributes significantly to lowering the risk relevance of a number of events, including loss of feedwater and small LOCAs.

(3) Fuel and Auxiliary Pools Cooling System (FAPCS)

The low pressure core injection (LPCI) mode of FAPCS is able to provide RPV makeup when water level drops in the RPV and pressure is at or below 0.689 MPa gauge (100 psig). The system injects water from the suppression pool and is manually initiated and provides an active backup to the Gravity Core Cooling System (GDCS).

The suppression pool cooling mode of FAPCS is another relevant function of the system that provides decay heat removal from the containment. This function is actuated automatically upon receipt of suppression pool high temperature.

(4) Reactor Water Cleanup/Shutdown cooling (RWCU/SDC)

The shutdown cooling mode of the RWCU of ESBWR is able to be placed in service at rated pressure and temperature conditions and continues during the entire shutdown period. The design of this system mode allows having RPV decay heat removal redundancy in all accident and transients scenarios both at high and low RPV pressure.

An important feature of this system for reducing risk is the addition of a third, diverse containment isolation valve that closes upon detection of a leak or break in the RWCU system.

(5) Depressurization System (DPV)

The DPVs provide a highly reliable means of depressurizing the RPV in the event of failure of the non-safety high or low pressure makeup systems. This permits core cooling with the safety related GDCS and reduces the frequency of high pressure core melt sequences.

(6) Passive Containment Cooling System (PCCS)

The PCCS provides passive containment heat removal following a LOCA or DPV actuation by continuously condensing steam in the containment and returning the condensate to the RPV via GDCS pools. This is a passive system designed with no components that need to change state within the first 24 hours of operation. The IC/PCC pools, in conjunction with the refueling pool, provide enough water inventory for decay heat removal beyond 72 hours.

One feature of the PCCS / GDCS combination that was included in the ESBWR design was a scupper on the interface between the GDCS and the upper drywell. This directs overflow from the GDCS pool to the suppression pool rather than allowing it to drain to the lower drywell. In scenarios in which GDCS does not operate as injection source, this minimizes the occurrence of exvessel fuel coolant interactions.

(7) Prevention of Intersystem LOCA

In SECY 90-016 and 93-087 it has been recommended that designers should reduce the possibility of a loss of coolant accident outside containment by designing (to the extent practical) all systems and subsystems connected to the Reactor Coolant System (RCS) to withstand full RCS pressure. All piping systems, major systems components (pumps and valves), and subsystems connected to the reactor coolant pressure boundary (RCPB) which extend outside the primary containment boundary are designed to the extent practicable to an ultimate rupture strength (URS) at least equal to full RCPB pressure. The design provisions provided reduce the possibility of an intersystem loss of coolant accident (ISLOCA) and consequently the probability of a loss of coolant accident outside the containment being an initiating event that could lead to core damage.

(8) Reactor Protection System (RPS)

The ESBWR has a highly reliable and diverse CRD scram system incorporating both hydraulic insert and electric run-in capabilities. The hydraulic scram system also includes additional backup scram valves to relieve scram air header pressure thereby causing the control rods to insert. Redundant and diverse scram signals are provided from the RPS and Alternate Rod Insertion (ARI) System to the hydraulic scram mechanisms and the electric run-in capability. This redundant and diverse scram capability significantly reduces the probability of an ATWS.

(9) Automatic Standby Liquid Control System (SLCS) and Feedwater Pump Trip

The standby liquid control system and feedwater pump trip provide backup reactor shutdown capability. Automatic initiation of the SLCS avoids the potential for operator error associated with manual SLCS initiation.

(10) Four Divisions of Safety Related Systems

There are four independent and separated divisions of safety related systems. Providing four passive divisions designed with single failure criteria substantially reduces the calculated CDF for events that require the actuation of safety related systems. Complete physical separation of electrical and mechanical divisions is important. Also the system piping that penetrates containment has been designed as an extension of containment.

(11) Two Onsite Diesel Generators (DG)

There are two independent and separated DGs, one dedicated to each of the two first line AC power systems (RWCU, FAPCS, etc.) and each capable of powering the complete set of normal safe shutdown loads in its division. This contributes significantly to lowering the risk relevance of Loss of Preferred Power transients.

(12) Four Divisions of Safety System Logic and Control (SSLC)

There are four divisions of self-testing SSLC instrumentation designed on the basis of two-out-of-four actuation logic. This configuration provides highly reliable initiation of ESF core cooling and heat removal systems. A four division two-out-of-four SSLC provides protection against inadvertent actuation in addition to assuring highly reliable actuation capability.

The ESBWR also incorporates a Diverse Protection System that is completely independent and diverse from SSLC and provides logic signals for actuation of some significant safety related systems (DPV, SRV, GDCS, ARI, and SCRAM). This diverse actuation system minimizes the possibility that common cause failures or software failures would prevent the safety related systems from operating.

In addition, the non-safety digital control systems provide a second diverse means of providing core and containment cooling via the PIP systems. In nearly all PRA scenarios, instrument and control failures can only cause core damage if all three diverse digital control systems fail to function. This provides a level of protection that drives the ESBWR CDF down to a very small value.

(13) Fire Protection System

The fire protection system can function to provide additional water to the ICC/PCC pools, and to provide a source of low pressure injection. The system was designed with a diesel driven pump that can operate independently of any other system in the plant. This provides another level of diversity in containment and core cooling.

The low pressure injection mode of fire protection does rely on some FAPCS valves to direct flow into the feedwater system. These valves have shown to be important in the shutdown and fire PRA analyses. One further insight would be to separate fire water injection from FAPCS injection so that this dependence would be removed.

19.4.3 Insights from Seismic Analysis

(1) Structures

Loss of structural integrity was considered to result in core damage. In this analysis, any one or more of these structural failures are conservatively presumed to result in core damage. The structures having the lowest seismic capacity are the reactor building and control building.

(2) DC Power

The failure of DC power results in core damage. Only passive safety systems were credited in the seismic analysis. These systems do not require AC power supply for their actuation. However DC power supply is required for a number of functions in those systems. The PCCS is the only fully passive system but it does require that depressurization valves actuate as well as GDCS and both systems have a dependency on the DC power supply. From this point of view the DC power supply has been considered separately in the event tree. In this system the most critical components are the batteries, cable trays and safety system components. Motor control centers were also included representing the panels that distribute DC and vital AC power. Failure of all DC power results in a high-pressure core melt because all control is lost, the isolation condensers fail, and the reactor cannot be depressurized.

The sequence with failure of DC power is dominated by the failure of the Motor Control Centers and DC distribution panels.

(3) Scram System

The failure to scram results in an ATWS. In this case there is a requirement for the opening of safety relief valves to prevent failure due to overpressure. The failure to open of safety relief valves SRVs) was assumed to lead to a core damage condition.

If SRV works properly then there is a need for the actuation of the Standby Liquid Control (SLCS) system in order to bring the reactor subcritical. The failure of this function will cause a core damage condition. The failure of control rods to insert is dominated by the relatively low seismic fragility of the fuel assemblies, control rod guide tubes, and housings.

Scram failure is dominated by the failure of the fuel assemblies and the failure of the accumulator tanks of the Standby Liquid Control System.

(4) Heat Exchangers

Failures of ICS and PCCS were dominated by failure of the heat exchangers.

19.4.4 Insights from Fire Analyses

(1) Fire Separation

The ESBWR due to its basic layout and safety design features is inherently capable of mitigating potential internal fires. Safety system redundancy and physical separation by fire barriers ensure that in all cases that one fire limits damage to one safety system division or DID system redundancy.

(2) Control Room and Remote Shutdown Panel Design

Fires in the control room have the capacity to affect the execution of human actions from there. One feature relevant to the design is that a fire in the control room does not affect the automatic actuation of the safety systems. Additionally, the existence of remote shutdown panels able to actuate heat removal systems allows the mitigation of the most relevant sequences to the long-term heat exchanger failure once there is an injection system working successfully.

19.4.5 Insights from Flooding Analyses

(1) Flood Separation

Safety system redundancy and physical separation for flooding by large water sources along with alternate safe shutdown features in buildings separated from flooding of safety systems give the ESBWR significant flooding mitigation capability

(2) Flood Mitigation Features

Due to the inherent ESBWR flooding capability discussed above, only a small number of flooding specific design features must be relied on to mitigate all potential flood sources. The flood specific features are: watertight doors on the Control and Reactor Buildings; floor drains in the Reactor and Control Buildings; CWS pump trip and valve closure on high water level in the condenser pit.

(3) Operator Actions

While timely operator action can limit potential flood damage, all postulated floods can be adequately mitigated (from a risk perspective) without operator action.

19.4.6 Suppression Pool Bypass and Ex-Containment LOCA Insights

The features that contribute to the prevention or mitigation of containment bypass were systematically reviewed to evaluate their specific contribution to containment bypass. Also, the core cooling features that could prevent or mitigate containment bypass were systematically reviewed to determine their contribution to total CDF. Those features that would increase the calculated CDF by more than a factor of 2, whether they failed or were not included in the design, were identified as important features.

The following features were identified as being the most significant contributors:

- Drywell-to-Wetwell Vacuum Breakers
- Redundant MSIVs
- Design and Fabrication of the SRV Discharge Lines
- Normally Closed Sample Lines and Drywell Purge Lines
- Diverse Reactor Water Cleanup System Isolation Valves

19.4.7 Shutdown PRA Insights

The evaluation examined the ability to remove decay heat and maintain inventory control for plant operation in shutdown modes, when there is fuel in the RPV. It included all aspects of the NSSS, the containment, and all systems that support operation of the NSSS and containment. It did not address events involving fuel handling outside the reactor building or fuel storage in the spent fuel pool.

The capabilities and features identified as being important to safety during shutdown are discussed below. They are separated into decay heat removal and inventory control functions.

19.4.7.1 Decay Heat Removal

(1) Isolation Condenser System (ICS)

During modes 3 and 4, the ICS is able to maintain reactor pressure and temperature within an acceptable range so that Safety/Relief valves will not open following isolation of the vessel.

(2) Reactor Water Cleanup / Shutdown Cooling System (RWCU/SDC)

RWCU/SDC has two trains in operation during the cooldown phase of shutdown (which is the most critical, as decay heat is still significant). However, one single train has enough decay heat removal capacity to maintain reactor pressure vessel temperature within acceptable limits. This means that no "fails to start" failure modes contribute to the frequency of the initiating events related to decay heat removal safety function.

(3) Water Inventory in Vessel and Reactor Building Upper Pools

The large amount of water stored in the vessel provides a reliable, passive heat sink during all phases of mode 5, increasing the time margin for operator actions. Once the reactor cavity has been flooded, water inventory in the reactor building upper pools further increases this protection.

(4) Gravity Driven Cooling System (GDCS)

GDCS does not rely upon cooling systems or external power, making it available to mitigate all initiating events considered.

(5) Injection Mode of Fire Protection System (FPS)

Though not a passive system, the FPS features redundant diesel engine powered pumps, allowing it to effectively mitigate Loss of Preferred Power and Loss of RCCWS/PSWS events.

19.4.7.2 Inventory Control

(1) LOCAs Inside Containment

Most of the risk during shutdown is associated with RWCU/SDC pipe or instrument line breaks in the drywell. These pipes are attached to the vessel below the top of fuel, so they provide a significant drain-down path. The only way to mitigate these accidents is for the water to flood up the containment to the elevation of the top of fuel. This can only be accomplished if the lower drywell hatches are closed.

During a refueling outage, it is expected that these hatches will be open for a significant fraction of the outage to allow work in the LDW. Care must be taken to provide a reliable means of closing these hatches following the initiation of a draindown event.

(2) LOCAs Outside Containment

LOCAs outside containment are shown to have negligible contribution to risk based in a number of ESBWR design features:

- These events can on only be due to RWCU/SDC piping, as this is the only system extracting reactor coolant from containment in mode 5, the rest of the RPV vessel piping being isolated.
- The RWCU/SDC containment penetrations have redundant, diverse and automatic power-operated containment isolation valves that close on signals from the leak detection and isolation system, the diverse protection system and the reactor protection system.
- The leak detection and isolation system, utilizing a two-out-of-four logic, will close the containment isolation valves on detection of high flow in the ASME Section III Class 1 portion of the RWCU/SDC piping system or on detection of high temperature in the Main Steam Tunnel. These independent methods provide a diverse means of detecting large breaks in the RWCU/SDC piping.
- A postulated break in the RWCU/SDC piping system inside the Reactor Building, which would otherwise allow reactor coolant to flow backwards through main feedwater lines and to spill into the Reactor Building, will be isolated by the redundant RWCU/SDC check valves even if a single failure of one check valve is assumed.
- The RWCU/SDCS in the ESBWR does not have the potential for diverting RPV inventory to the suppression pool through SP suction, return or spray lines. In addition, the absence of recirculation lines in the ESBWR design further reduces the potential RPV draining paths.

19.4.8 Insights from Level 2 Severe Accident Analyses

In the event of a core damage accident, the ESBWR containment has been designed with specific mitigating capabilities. These capabilities not only mitigate the consequences of a severe accident but also address uncertainties in severe accident phenomena. The capabilities are listed below along with a discussion of the specific severe accident phenomena that the mitigation device is addressing.

(1) AC-Independent Fire Water Addition System

This Fire Protection System (FPS) and Fuel and Auxiliary Pools Cooling System (FAPCS) not only play an important role in preventing core damage through common lines but they are the backup source of water for flooding the lower drywell should the core become damaged and relocate into the containment (primary source is the deluge subsystem pipes of Gravity Driven Cooling System). The primary point of injection for these systems is the LPCI injection, through feedwater pipeline, to the reactor pressure vessel. Flow can also be delivered through the drywell spray header to the drywell. The drywell spray mode of this system not only provides for debris cooling, but it is capable of directly cooling the upper drywell atmosphere and scrubbing airborne fission products.

(2) Containment Inerting System Bleed line

The Containment Iterating System bleed line has air operated valves mounted in a line that connects the wetwell airspace to the reactor building HVAC discharge. This system will provide for a scrubbed release path in the event that pressure in the containment cannot be maintained below the structural limit. The path can be opened or closed at pressure up to the ultimate capability of the containment.

(3) Vessel Depressurization

The RPV depressurization system can prevent the effects of direct containment heating (DCH) from high pressure melt ejection. If the reactor vessel would fail at an elevated pressure, fragmented core debris could be transported into the upper drywell. The resulting heat up of the upper drywell could pressurize and fail the drywell. The ESBWR has many diverse means of depressurizing the vessel and preventing this situation.

(4) Inerted Containment

One of the important severe accident consequences is the generation of combustible gases. Combustion of these gases could increase the containment temperature and pressure. The ESBWR containment will be inerted during operation to minimize the impact from the generation of these gases.

(5) Containment Isolation

The ESBWR containment design minimizes the number of penetrations. This impacts the severe accident response due to a smaller probability of containment isolation failure. All lines which originate in the reactor vessel or the containment have dual barrier protection which is generally obtained by redundant isolation valves.

(6) Upgraded Low Pressure Piping

The low pressure piping that could see RPV pressure has been upgraded to withstand higher pressure. This reduces the probability of an interfacing system LOCA and the severe accident consequences associated with such an event.

(7) Drywell-Wetwell Vacuum Breakers

The ESBWR contains three vacuum breakers which provide positive position indication in the control room. Failure of the vacuum breakers to close as designed can potentially lead to increased source terms and early containment failure. If the operators have indication that any of the vacuum breakers has failed or is leaking, there is a built in provision to isolate the failed component. The vacuum breakers have been located high in the wetwell to reduce potential loads occurring during pool swell. The vacuum breaker design in the ESBWR reduces the potential for suppression pool bypass.

(8) Overall Containment Performance

The containment is designed to withstand the generation of 100% metal water reaction of the clad surrounding the fuel. The ultimate strength capability is important for very rapid containment challenges such as direct containment heating and rapid steam generation.

(9) Basemat Internal Melt Arrest and Coolability device (BiMAC)

ESBWR design uses a passively-cooled boundary that is impenetrable by the core debris in whatever configuration it could possibly exist on the lower drywell (LDW) floor. For ex-vessel implementation, this boundary is provided by a series of side-by-side inclined pipes, forming a jacket which can be effectively and passively cooled by natural circulation when subjected to thermal loading on any portion(s) of it. Water is supplied to this device from the GDCS pools via a set of squib-valve-activated deluge lines. The timing and flows are such that (a) cooling becomes available immediately upon actuation, and (b) the chance of flooding the LDW prematurely, to the extent that this opens up a vulnerability to steam explosions, is very remote. The jacket is buried inside the concrete basemat and would be called into action only in the event that some or all of the core debris on top is non-coolable.

Analyses have shown that the containment will not fail by Basemat melt-through or by overpressurization as long as the BIMAC functions.

19.4.9 Severe Accident Mitigation Design Alternatives (SAMDAs)

19.4.9.1 Introduction and Background

The term "severe accident" refers to those events which are "beyond the substantial coverage of design basis events" and includes those for which there is substantial damage to the reactor core whether or not there are serious off-site consequences, see Severe Accident Policy Statement, 50 Fed.Reg. 32,138,32,139 (August 8,1985). For new reactor designs, such as the ESBWR, the Nuclear Regulatory Commission (NRC), in satisfaction of its severe accident safety requirements, is requiring, among other things, the evaluation of design alternatives to reduce the radiological risk from a severe accident by preventing substantial core damage (i.e., preventing a severe accident) or by limiting releases from the containment in the event that substantial core damage occurs (i.e., mitigating the impacts of a severe accident).

The Commission's severe accident safety requirements for new designs are set forth in 10 CFR Part 52, paragraph 52.47(a) (1) (ii), (iv) and (v). Paragraph 52.47(a) (1) (ii) references the Commission's Three Mile Island safety requirements in 10 CFR 50.34(f). Paragraph 52.47 (a) (1) (iv) concerns the treatment of unresolved safety issues and generic safety issues. Paragraph 52.47 (a) (1) (v) requires the performance of a design-specific probabilistic risk assessment (PRA). The Severe Accident Policy Statement elaborates what the Commission is requiring for new designs. The Safety Goal Policy Statement sets goals and objectives for determining an acceptable level of radiological risk.

GE performed a probabilistic risk assessment (PRA) for the ESBWR design to achieve the following objectives:

- Identify the dominant severe accident sequences and associated source terms for the design.
- Modify the design, on the bases of PRA insights, to prevent or mitigate severe accidents and reduce the risk of severe accidents.
- Provide a basis for concluding that all reasonable steps have been taken to reduce the chances of occurrence, and to mitigate the consequences, of severe accidents.
- Provide a basis for concluding that the NRC safety goals are met by the plant design.

The ESBWR PRA analysis is provided in NEDO-33201. The PRA was performed in accordance with the requirements of 10 CFR 52 and 10 CFR 50.34(f)(1)(i) which requires the performance of a plant/site-specific probabilistic risk assessment, the aim of which is to seek such improvements in the reliability of core and containment heat removal systems as are significant and practical and do not impact excessively on the plant.

The U.S. Court of Appeals decision, in Limerick Ecology Action v. NRC, 869 F.2d 719 (3rd Cir. 1989), effectively requires the NRC to include consideration of certain SAMDAs in the environmental impact review performed under Section 102(2)(c) of NEPA.

These two requirements share a common purpose to consider alternatives to the proposed design, to evaluate potential alternative improvements in the plant design that increase safety performance during severe accidents, and to prevent reasonable alternatives from being foreclosed. As a matter of discretion, the Commission has determined that considering SAMDAs is consistent with the intent of 10 CFR Part 52 for early resolution of issues, finality of design issues resolution, and achieving the benefits of standardization.

Recently, the NRC Staff expanded the concept of SAMDAs to encompass design alternatives to prevent severe accidents, as well as mitigate them. See NUREG-1437, "Generic Environmental Impact Statement for License Renewal of Nuclear Plants," (Volume I, p. 5-100). By doing so, the Staff makes the set of SAMDAs considered under NEPA the same as the set of SAMDAs considered in satisfaction of the Commission's severe accident requirements and policies.

19.4.9.2 Purpose

The purpose of this subsection is to demonstrate that all cost effective steps have been taken to reduce the risk associated with operation of plants of ESBWR design. The basis for determining the status of severe accident closure under NEPA for the ESBWR design is also provided. The document supports a determination, which could be codified in a manner similar to the format of the Waste Confidence Rule (10 CFR § 51.23) as proposed amendments to 10 CFR Part 51. These amendments would provide that:

- For the ESBWR design all reasonable steps have been taken to reduce the occurrence of a severe accident involving substantial damage to the core and to mitigate the consequences of such an accident should one occur. Additionally, all reasonable steps were taken to reduce the radiological environmental impacts from normal reactor operations, including expected operational occurrences, to as low as reasonably achievable (ALARA).
- No further cost-effective SAMDAs to the ESBWR design have been identified to mitigate the consequences of or prevent a severe accident involving substantial damage to the core; and,
- No further evaluation of severe accidents for the ESBWR design, including SAMDAs to the design, is required in any environmental report, environmental assessment, environmental impact statement or other environmental analysis prepared in connection with issuance of a combined license for a nuclear power plant referencing a certified ESBWR design.

The evaluation presented in this document is modeled after that found in the Limerick and Comanche Peak NEPA/SAMDA Final Environmental Statement (FES) Supplements for those facilities. Additional information concerning the radiological risk from severe accidents for those plants is not found in the supplements, but in the FESs for the Limerick and Comanche Peak facilities. That information with respect to the ESBWR design is presented in this document. The discussion herein of the radiological risk from severe accidents is based on the ESBWR PRA (NEDC-33201).

19.4.9.3 Evaluations of Radiological Risk from Nuclear Power Plants

19.4.9.3.1 Evaluation of SAMDAs under NEPA and Limerick Ecology Action

Limerick Ecology Action stands for two propositions. First, that NEPA requires explicit consideration of SAMDAs unless the Commission makes a finding that the severe accidents being mitigated are remote and speculative. Second, that the Commission may not make this finding and dispose of NEPA consideration of SAMDAs by means of a policy statement. The purpose of evaluating SAMDAs under NEPA is to assure that all reasonable means have been considered to mitigate the impacts of severe accidents that are not remote and speculative. As discussed above, the Commission has indicated that it will resolve the NEPA/SAMOA issue in the same proceeding, called a unitary proceeding, in which it certifies a new reactor design.

The Commission's Severe Accident and Safety Goal policy statements require the Commission to make certain findings about each new reactor design. For evolutionary designs, of which the ESBWR is one, this must be done by the Staff in conjunction with FDA approval and by the Commission in conjunction with certification. First, the Commission must find that an evolutionary plant meets the safety goals and objectives; i.e., that the radiological risk from operating an evolutionary plant will be acceptable, meaning that any further reduction in risk will not be substantial.

Second, the Commission must find that all reasonable means have been taken to reduce severe accident risk in the evolutionary plant design. As part of the basis for making this finding, the cost-effectiveness of risk reduction alternatives of a preventive or mitigative nature must be evaluated.

19.4.9.3.2 Cost/Benefit Standard for Evaluation of SAMDAs

The NRC updated its recommended approach for the monetary conversion of radiation exposures. Previous guidance specified that 1 person-rem of exposure should be valued at $1000. This conversion factor for offsite doses was intended to account for both health effects and offsite property damage, and exposures incurred in future years were not to be discounted. The guidance given in the NRC's regulatory analysis guidelines (NUREG/BR-0058, Revision 2), recommends using $2000 per person-rem of exposure as the monetary conversion factor. In addition, future exposures are to be discounted to arrive at their present worth to assess values and impacts. Offsite property damage from nuclear accidents is to be valued separately, and is not part of the $2000 per person-rem value. A criterion of $3000 per person-rem averted was added to account for offsite property damage and other related costs for severe accidents.

19.4.9.3.3 Socio-Economic Risks for Severe Accidents

Environmental Impact Statements (EIS) for nuclear power plants provide separate, general discussions of the socio-economic risks from severe accidents. In keeping with this precedent, a general discussion of socio-economic risks for the ESBWR design, based in large measure on the discussion of such risks in NUREG-1437, "Draft Generic Environmental Impact Statement for License Renewal of Nuclear Plants" is provided in the remainder of this subsection.

The term "socio-economic risk from a severe accident" means the probability of a severe accident multiplied by the socio-economic impacts of a severe accident. "Socio-economic impacts" in turn relate to off-site costs. The off-site costs considered in NUREG-1437 (see Vol. 1 at 5-90) are:

- evacuation costs,
- value of crops or milk, contaminated and condemned,
- costs of decontaminating property where practical,
- indirect costs due to the loss of the use of property or incomes derived there from (including interdiction to prevent human injury), and
- impacts in wider regional markets and on sources of supply outside the contaminated area.

NUREG-1437 estimated the socio-economic risks from severe accidents. The estimates were based on 27 FESs for nuclear power plants that contain analyses considering the probabilities and consequences of severe accidents. For these plants, the off-site costs were estimated to be as high as $6 billion to $8 billion for severe accidents with a probability of once in one million operating years. Higher costs were estimated for severe accidents with much lower probabilities. The projected costs of adverse health effects from deaths and illnesses were estimated to average about 10-20% of off-site mitigation costs and were not included in the $6-$8 billion dollar estimate.

Another source of costs, which NUREG-1437 indicated could reach into the billions of dollars, were costs associated with the termination of economic activities in a contaminated area. This could create adverse economic impacts in wider regional markets and sources of supplies outside the contaminated area. The predicted conditional land contamination was estimated to be small (10 acres/year at most), see NUREG-1437, pp. 5-90 through 5-93.

NUREG-1437 provides the bases for the Commission's proposed amendments to 10 CFR Part 51 concerning the environmental impacts of license renewal. The proposed amendments find that the socio-economic risks from severe accidents are predicted to be small and the residual impacts of severe accidents so minor that detailed consideration of mitigation alternatives is not warranted, see 56 Fed. Reg. 47,016, 47,019, 47,034-35 (September 17, 1991).

The socio-economic risks contained in NUREG-1437 are bounding for plants of ESBWR design. First, the core damage frequency for plants of ESBWR design is less than 10^{-7} per year. Thus, no accidents, and hence no off-site costs, are expected at probabilities at or greater than once in one million years. Second, plants of ESBWR design meet the safety goals set forth by the NRC.

19.4.9.4 Radiological Risks

19.4.9.4.1 Radiological Risk from Normal Operations of an ESBWR Plant

In addition to specifying numerical limits, Appendix I also requires an applicant to include in the radwaste system "all items of reasonably demonstrated technology that, when added to the system sequentially and in order of diminishing cost/benefit return can for a favorable cost/benefit ratio, effect reductions in dose to the population expected to be within 50 miles of the reactor". The standard to be used in making this assessment is the cost/benefit ratio of $2000 per person-rem averted.

The ESBWR design complies with the guidance of Appendix I, therefore further consideration of alternatives to reduce the radiological risks from normal operation of a plant of ESBWR design is not warranted in order to satisfy NEPA. Moreover, the radiological impacts from normal operation of an ESBWR are environmentally insignificant.

Non-radiological impacts from operation of an ESBWR plant include those from the circulating system which removes heat from the reactor (e.g., cooling towers, cooling lakes, etc.), intake systems for the water in the circulating systems, discharge systems for the water in the circulating system, biocide treatment in circulating water to prevent fouling by organisms, chemical waste treatment and disposal, sanitary waste treatment system, and electrical transmission facilities. Each of these systems is part of that portion of the ESBWR design which is not being certified because it is site-specific.

It may be appropriate to consider design alternatives for non-radiological systems under NEPA. However, the choice of alternatives will not have an effect on the portion of the ESBWR design that is being certified. Consideration of alternative designs to systems affecting non-radiological impacts must be done on a site-specific basis. Sections 50.34a and 50.36a of 10 CFR Part 50 require, in effect, that nuclear power reactors be designed and operated to keep levels of radioactive materials in gaseous and liquid effluents during normal operations, including expected operational occurrences, "as low as reasonably achievable" (ALARA). Compliance with the guidelines in Appendix I to 10 CFR Part 50 is deemed a conclusive showing of compliance with these ALARA requirements.

19.4.9.4.2 Severe Accidents in Plants of ESBWR Design

NEDC-33201 establishes that the Commission's severe accident safety requirements have been met for the ESBWR design, including treatment of internal and external events, uncertainties, performance of sensitivity studies, and support of conclusions by appropriate deterministic analyses and the evaluations required by 10 CFR Part 50.34(f). It also establishes that the Commission's safety goals have been met.

Specifically, the following topics were addressed in NEDC-33201:

- Consideration of the contributions of internal events and external events to severe accident risks, including a seismic risk analysis based on the application of the seismic margins methodology;
- Identification of the ESBWR dominant accident sequences;

Section 19.1 of Chapter 19 of the ESBWR DCD addresses how the goals of the Severe Accident Policy Statement have been met for plants of ESBWR design.

Specific conclusions concerning severe accidents for plants of ESBWR design based on the NEDC-33201 evaluations are as follows:

- Core Damage Frequency: The ESBWR core damage frequency was determined to be less than 1E-7 per reactor year. Individual Risk (Prompt Fatality Risk). The prompt fatality risk to a biologically average individual within one mile of an ESBWR site boundary was determined to be significantly less than the goal of one-tenth of one percent of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. Population are generally exposed.

- Societal Risk (Latent Fatality Risk): The latent fatality risk to the population in the vicinity of an ESBWR was determined to be significantly less than the goal of one-tenth of one percent of the sum of the cancer fatality risks resulting from all other causes.
- Probability of Large Off-Site Dose: The probability of exceeding a whole body dose of 25 rem at a distance of one-half mile from a ESBWR was determined to be less than 1E-8 per reactor year.

19.4.9.4.3 Dominant Severe Accidents Sequences for Plants of ESBWR Design

In performing the PRA for the ESBWR design, GE identified and evaluated many severe accident sequences. For each sequence, the analysis identified an initiating event and traced the accident's progression to its end. For sequences involving core damage, offsite consequences were estimated.

Only the sequences with frequencies greater than 1E-9 per reactor year were considered. The complete radiological consequence analysis of the dominant sequences can be found in NEDC-33201.

Sequences with probabilities of occurrence less than 1E-9 were considered remote and speculative. While the Commission has not yet specified a quantitative point at which it will consider severe accident probabilities as remote and speculative, it has indicated that a decision to consider severe accidents remote and speculative would be based upon the accident probabilities and the accident scenarios being analyzed. See Vermont Yankee Nuclear Power Corporation, (Vermont Yankee Nuclear Power Station), CLI-90-07, 32 NRC 129, 132 (1990). GE believes that the severe accident analysis in NEDC-33201 provides a sufficient basis for the Commission to find that ESBWR sequences with frequencies less than 1E-9 per reactor year can be deemed remote and speculative.

19.4.9.4.4 Overall Conclusions from the ESBWR PRA

The specific conclusions about severe accident risk discussed above support the overall conclusion that the environmental impacts of severe accidents for plants of ESBWR design represent a low and acceptable risk to the population and to the environment. For the ESBWR design, all reasonable steps have been taken to reduce the occurrence of a severe accident involving substantial damage to the core and to mitigate the consequences of such an accident should one occur. No further cost-effective modifications to the ESBWR design have been identified to reduce the risk from a severe accident involving substantial damage to the core. No further evaluation of severe accidents for the ESBWR design is required to demonstrate compliance with the Commission's severe accident requirements or policy, SECY-90-016 or the EPRI ALWR Utility Requirements Document.

19.4.9.5 Cost/Benefit Evaluation

19.4.9.5.1 SAMDA Definition Applied to Plants of ESBWR Design

This subsection considers whether the ESBWR design should be modified in order to prevent or mitigate the consequences of a severe accident in satisfaction of the NRC's severe accident requirements in 10 CFR Parts 50 8c 52 and the Severe Accident Policy Statement. The cost/benefit evaluation of SAMDAs to plants of ESBWR design uses the expanded definition of

SAMDAs, design alternatives that could prevent and/or mitigate the consequences of a severe accident.

19.4.9.5.2 Cost/Benefit Standard for Evaluation of ESBWR SAMDAs

As discussed earlier, the cost/benefit ratio of $2,000 per person-rem averted is viewed by the NRC and the nuclear industry as an acceptable standard for the purposes of evaluating SAMDAs. This standard was used as a surrogate for all off-site costs in the cost/benefit evaluation of SAMDAs to plants of ESBWR design. In order to accurately reflect the costs associated with prevention of severe accidents, averted on-site costs were incorporated for SAMDAs that were at least partially preventative in nature. On-site costs resulting from a severe accident include replacement power, on-site cleanup costs, and economic loss of the facility.

The equation used to determine the cost/benefit ratio is:

$$R = \frac{\text{Cost of SAMDA Implementation — Averted On-Site Costs}}{\text{Reduction in Residual Risk}}$$

A plant life time of 60 years was assumed to maximize the reduction in residual risk.

19.4.9.5.3 Cost Estimates of Potential Modifications to the ESBWR Design

All previous evaluations of design alternatives (e.g., the Limerick and Comanche Peak FES Supplements, NUREG-1437, and the ABWR SSAR) have reported design alternative costs which, at a minimum, are in the hundreds of thousands of dollars. The high cost of design alternatives which have the potential to proved risk reduction is also demonstrated in several state-of-the-art surveys (e.g., NUREG/CR-3908, NUREG/CR-4025 and NUREG/CR-4920). In fact, most proposed design alternatives cost in the millions of dollars to implement.

This analysis uses a representative design alternative implementation cost of $200,000 (which is below the cost of all design alternatives which would be expected to provide a non-negligible reductions in risk) to determine if additional analysis needs to be performed for plants of ESBWR design.

For design alternatives which can prevent core damage, averted on-site costs will also be considered. A conservative estimate of averted on-site costs can be obtained by multiplying the frequency of core damage, the number of years the plant will be licensed to operate, and the sum of plant construction cost and cleanup costs. By assuming a plant life of 60 years, a construction cost of $3B and cleanup costs of $3B and an implementation cost of $200,000, the resulting frequency of core damage would be about 5.6E-7. The frequency of core damage from the ESBWR PRA is about an order of magnitude less than this value. Therefore the implementation of a design alternative which would have an impact on the core damage frequency would have to cost significantly less than $200,000, which is not deemed likely.

19.4.10 Summary and Conclusions

ESBWR design alternatives that only provide severe accident mitigation must cost significantly less than the $200,000, which is the minimum cost for a design alternative that has the potential for a measurable reduction in severe accident risk. This low cost limitation is a result of the ESBWR providing adequate protection to the public and the environment. A detailed analysis of specific design alternatives is not warranted because the cost limitations are so low. Therefore, plants of the ESBWR design do not require additional SAMDA evaluation.

19.4.11 References

19.4-1 Assessment of Severe Accident Prevention and Mitigation Features, NUREG/CR-4920, Brookhaven National Laboratory, July 1988.

19.4-2 Design and Feasibility of Accident Mitigation Systems for Light Water Reactors, NUREG/CR-4025, R&D Associates, August 1985.

19.4-3 Evaluation of Proposed Modifications to the GESSARII Design, NEDE 30640, Class III, GE Nuclear Energy, San Jose, CA, June 1984.

19.4-4 Generic Environmental Impact Statement for License Renewal of Nuclear Plants, NUREG-1437, Draft for Comment.

19.4-5 "Issuance of Supplement to the Final Environmental Statement - Comanche Peak Steam Electric Station, Units 1 and 2", NUREG-0775 Supplement, December 15, 1989.

19.4-6 Severe Accident Risks: An Assessment fro Five US Nuclear Power Plants, NUREG-1150, January 1991.

19.4-7 "Supplement to the Final Environmental Statement - Limerick Generating Station, Units 1 and 2", NUREG-0974 Supplement, August 16, 1989.

19.4-8 Survey of the State of the Art in Mitigation Systems, NUREG/CR-3908, R&D Associates, December 1985.

19.4-9 Technical Guidance for Siting Criteria Development, NUREG/CR-2239, Sandia National Laboratories, December 1982.

19.4-10 Title 10, Code of Federal Regulations, Part 50 and 52.

19.4-11 50FR32138, Policy Statement on Severe Reactor Accidents Regarding Future Designs and Existing Plants, August, 1985.

19.5 PRA-BASED RELIABIITY, AVAILABILITY AND MAINTAINABILITY

In this section, the results of the PRA are reviewed to determine the appropriate reliability and maintenance actions to be considered throughout the life of an ESBWR plant so that the PRA remains an adequate basis for quantifying plant safety. These actions comprise a part of the plant's reliability assurance program (RAP) comprising operating and maintenance procedures required by Standard Review Plan (SRP) Subsection 13.5.2.

19.5.1 General Approach

The PRA is reviewed to determine the relative importance of prevention and mitigation features of the ESBWR in satisfying the key PRA measures of core damage frequency (CDF) and frequency of offsite release. Also considered are the initiating events that have a significant impact on CDF. This review allows the most important plant features to be identified.

Maintenance of SSC groups identified in this section is intended to preserve the PRA measures calculated in NEDC-33201P. Section 19.6 provides the identification of equipment necessary to meet the PRA and severe accident goals.

19.5.2 Important Structures, Systems and Components (Level 1)

To determine which plant structures, systems and components (SSCs) are the most important with respect to CDF, the Level 1 analysis results are analyzed. The SSCs are listed in order of Fussell-Vesely (FV) importance, or the percent of cutsets that contribute to the CDF, as calculated by the CAFTA code. A second criterion for selecting SSCs is to consider those SSCs with high "risk achievement worth", or the increase in CDF if that SSC always fails. The identified SSCs are grouped by similarity of the functions performed. The 10 groups of SSCs of greatest importance, in that they had FV importance greater than 1% or a risk achievement worth greater than 5 are considered for the RAM program. Human actions are not considered part of this program. The group of components within the control of the COL applicant that are of significance to limiting the CDF are the scram related I&C components, the essential batteries, and the Drywell/Wetwell Vacuum Breakers Considering the potential unavailability impact, the Depressurization and the Gravity Driven Cooling System actuation valves are considered. The COL applicant should assure that maintenance and test activities for these components are appropriate to assure high reliability and availability.

The relative importance of some ESBWR features is not established by the Level 1 analysis described above because some important SSCs are not treated in the Level 1 calculation. To identify other important SSCs, the Level 2, seismic, fire, flood and shutdown analysis results are reviewed and discussed below.

19.5.3 Important Structures, Systems and Components (Level 2)

The Level 2 analysis evaluates the probability of offsite release of fission products following core damage. Those analyses related to the consequences of core damage were reviewed, including source term sensitivity studies, deterministic analysis of plant performance, and containment event trees. Those systems that would be important with regard to mitigating a core damage event were considered as potential risk-significant SSCs.

The following features were identified:

- The Automatic Depressurization System (ADS)

  The DPVs and SRVs are important SSCs for the ADS because they are the components that function to release steam to reduce RPV pressure

- The Containment Venting function of Containment Inerting System

  The SSCs identified by the analysis are the Containment Inerting system bleed valves, which prevent containment failure and limit offsite doses after core damage.

19.5.4 Important Structures, Systems and Components (Seismic)

The primary containment and the Reactor Building are the Category I structures in the design certification scope with the lowest values of HCLPF, but because both have HCLPF greater than 1.1 no special RAP activities are deemed necessary for these structures. Other SSCs identified by the seismic analysis as being important are as follows:

- The motor control centers of the emergency DC distribution System
- The heat exchangers of the Passive Containment Cooling System and the Isolation Condenser System
- The Fuel Assemblies and Hydraulic Control Units
- The SLC tank of the Standby Liquid Control System
- The diesel-driven pump of the Fire Water System

19.5.5 Important Structures, Systems and Components (Fire)

The fire risk analysis considers the potential for core damage from plant damage resulting from a fire. The important SSCs identified by this analysis are the room fire barriers, which prevent the fire from spreading to other rooms, barriers that separate each division of class 1E safety systems and also separate redundant equipment of defense in depth systems, the Smoke Removal System, which maintains pressure differentials to exhaust smoke rather than allow it to reach other areas, and the remote shutdown panel and control which are needed following a fire in the control room or HVAC failure in the control room.

19.5.6 Important Structures, Systems and Components (Flood)

The flood risk analysis considers the potential for core damage from plant damage resulting from a flood. The important SSCs identified by this analysis are the watertight doors in the Control and Reactor Buildings that separate each division of class 1E safety systems, floor drains in the Reactor and Control Buildings, Circulating Water System (CIRC) pump trip and valve closure on high water level in the turbine building condenser pit and anti-siphon capability, which limit the amount of water spilled into the reactor or fuel building.

19.5.7 Important Structures, Systems and Components (Shutdown)

The shutdown risk analysis considers the potential for core damage during shutdown. Potential core damage during shutdown arises when the decay heat removal or inventory control functions are lost. The cutsets equation giving the Core Damage Frequency for shutdown modes has been analyzed in terms of Fussell-Vesely importance measure, to determine which structures, systems and components contribute most to the shutdown risk. The important SSCs identified by this analysis are the Gravity Driven Cooling System actuation valves in the injection and equalizing lines, the diesel generators as well as some electrical components such as breakers needed to transfer loads to the diesel generators, the common cause failure of the station emergency batteries of the DC Power Supply System, the injection mode of the Fire Protection System, particularly the adequate alignment of the FAPCS to allow FPS flow to reach the vessel, and the Reactor Component Cooling Water System pneumatic valves regulating the flow through the heat exchangers.

19.5.8 Important Systems with Redundant Trains

Several plant systems have multiple trains of which only one is required to operate to perform the system safety function, the other trains providing redundancy. Because of this redundancy, components of the systems may not show up in a listing of high importance components. However, it is possible that operation or maintenance activities related to these systems could introduce some common cause failures which could affect all similar trains of a given system and, thereby, render all trains of such systems incapable of performing their safety functions. Engineering judgment is used to identify the multiple train systems having important safety functions that should be checked in addition to any identified component tests or maintenance. The systems selected are the essential AC and DC Electrical System, the Isolation Condenser (IC) System, the Drywell/Wetwell Vacuum Breakers, the Standby Liquid Control System (SLCS), the Depressurization Valves (DPV), the Gravity Driven Cooling System (GDCS), the Reactor Water Cleanup System in the shutdown cooling mode (RWCU/SDC), the Fuel and Auxiliary Pools Cooling (FAPCS) System in the suppression pool cooling and low pressure injection mode, the Reactor Component Cooling Water (RCCWS) System, the Plant Service Water (PSWS) System, and the Instrument Air System (IAS).

19.5.9 Important Capabilities Outside the Control Room

Most safety-related actions by plant operators are conducted from inside the control room. However, in some sequences it is necessary for the operators to take appropriate action from stations outside the control room. Engineering judgment was used to identify activities that the operators should be capable of performing outside the control room, during internal flood, during reactor shutdown, or when the control room is inaccessible, such as in event of a fire.

The identified activities outside the control room are:

- Manual alignment of the CRD or FAPCS systems for RPV injection if required
- Execution of procedures for operating the remote shutdown panels
- Closing water tight doors that are open before opening doors to attempt corrective action
- Manual alignment of the Firewater System for make-up of the IC/PCC pools and for RPV injection through FAPCS and FW lines after a seismic event
- Connection of the fire truck for make-up of the IC/PCC pools after a seismic event
- Check lower drywell personnel and equipment hatches are closed (or close them if they are open) in the case of a RPV draining event during shutdown

19.5.10 Reliability and Maintenance Actions

The individual SSCs identified as being “important” were reviewed to determine the appropriate reliability and maintenance actions. These actions are defined in this subsection.

Component Inspections and Maintenance

The group of component types with the highest FV importance in the Level 1 analysis are common cause failure of scram related I&C components. Safety-related I&C systems have a built-in self test that checks circuits frequently. In addition, one of four of most of these types of components can be bypassed and tested during plant operation without loss of system function. Such tests provide a complete simulation of the signals, more than what is included in the self-test. During plant outages, it is possible to run more detailed tests, including a complete system test and identification of signal errors.

Common-cause miscalibration of redundant system sensor and transmitters, and of RPV Level and pressure sensors, and common-cause failure (CCF) of digital trip modules (DTMs), will have acceptable probabilities if adequate administrative controls are exercised. The procedure for testing should include a warning about their importance to safety

Reliability of offsite power sources cannot be completely controlled by the plant. However, to assure that plant equipment does not contribute to power losses, inspection of switchyard equipment should be performed with a frequency of at least once every six months in accordance with site administrative procedures.

The next system components of greatest FV importance are the essential batteries (CCF). Station emergency batteries receive adequate periodic checks in accordance with plant Technical Specifications.

The CCF and independent failures of depressurization and safety relief valves (SRVs) can be kept to an acceptably low probability if the SRVs receive the appropriate in-service inspection, The SRV control panel can also be tested, separate from valve operation, to assure that it works properly.

The CCF and independent failures of DW-WW vacuum breaker (VB) to close can be kept to an acceptably low probability if the VBs receive the appropriate in-service inspection.

IC and PCC System Testing

Redundant motor operated valves interconnecting reactor well pool with IC/PCC pools to extend water inventory from 24 to 72 hours have been identified as significant components. The RAP activities are aimed at ensuring by periodical testing and more extensively during refueling that the components' reliabilities are maintained as required. Checking of heat exchanger performance requirements shall also be performed.

Depressurization

The ADS technical specifications are adequate and no additional actions are needed.

Batteries and AC Uninterruptible power supplies

Station emergency batteries and AC Uninterruptible power supplies will receive adequate periodic checks in accordance with plant Technical Specifications.

GDCS System

The testable GDCS check valves shall be tested quarterly to ensure the disk readiness to function, both to open, if required, and to close in case of spurious opening of the actuation valves.

During bi-annual refueling, an inspection of the strainers of the GDCS equalizing lines connected to the suppression pool shall be performed to prevent potential undetected obstructions.

The following activities are suggested for RAP:

- The ten fusible plug valve flanges and outlets should be inspected during every refueling outage to assure there is no leakage
- Two of ten fusible plug valves should be removed, inspected and their temperature setpoints tested every other refueling outage

AC-Independent Firewater System

Lining up the firewater should be specifically included in the training programs to assure that the system benefits are obtained. Specific procedures are required to be developed by the COL applicant to align the Fire Protection System (FPS) for vessel injection or IC/PCC makeup.

It is recommended that key components are tested to ensure that pumps and valves are operable and that there is no significant flow blockage in the flow paths from the Fire Water System to the reactor pressure vessel and to the drywell spray.

Venting Function

The Venting function is identified in Subsection 19.4 as important to limiting fission product release. System flow testing and special operator training should also be considered for inclusion in the RAP.

Seismic-Related Inspections

The seismic capability of the following equipment items is identified as risk-significant:

- The motor control centers of the emergency DC Distribution System
- The heat exchangers of the Passive Containment Cooling System and the Isolation Condenser System
- The Fuel Assemblies and Hydraulic Control Units
- The SLC tank, of the Standby Liquid Control System
- The diesel-driven pump of the Fire Water System

For this equipment, seismic related inspections should be conducted after any earthquake equal to or greater than that corresponding to the cumulative absolute velocity (CAV) shutdown threshold.

Plant Structures

No maintenance activities other than those already associated with the in-service surveillance of the seismic instruments are needed for seismic events.

Hydraulic Control Units and Control Rod Drives

No additional reliability and maintenance actions are needed beyond those contained in technical specifications.

On-Site Diesel Generators

Maintaining diesel generator reliability is a basic part of the maintenance rule (10CFR50.65). A reliability assurance program is required which maintains a target reliability.

Fire Protection

The room fire barriers, the Smoke Removal System, and the remote shutdown panel and control were determined to be relatively important. Fire barriers, including penetrations, should be inspected periodically to assure that they retain their integrity with respect to confining a fire. The Smoke Removal System should be operated annually to demonstrate that it is able to maintain a negative pressure in a room with a fire so that probability of propagation of fire and/or smoke to other rooms is low.

The remote shutdown panel is tested periodically to show that it can perform its functions that will lead to safe shutdown.

Flood Protection

Periodically, room water barriers should be inspected to ensure that they will prevent the spread of flooding; room drain lines should be checked to ensure no blockage exists; CIRC isolation valves (MOVs) should be stroke tested; the ability of CIRC pump circuit breakers to trip upon receipt of a trip signal should be demonstrated; and level sensors in the turbine building must be periodically tested to show their functionality.

Shutdown Protection

The GDCS is of importance to shutdown risk, especially the actuation valves. The reliability and maintenance actions proposed earlier are considered adequate from the shutdown risk point of view. Carrying out maintenance on GDCS components during mode 5 when reactor cavity has not been flooded should be strongly discouraged.

With regard to the diesel generators and sequencing breakers, the comments made earlier are also relevant from the shutdown risk point of view.

Given the high contribution of LOPP to shutdown PRA, inspection and testing of AC-independent fire protection system in vessel injection mode should be included in RAP. Earlier comments regarding training and procedures for manual alignment are applicable to shutdown risk as well.

The analysis of loss of reactor coolant inventory control function during mode 5 performed within the shutdown PRA clearly underscores the importance of keeping the lower drywell personnel and equipment hatches closed as long as possible. Indeed, a break below the level of the core (in RWCU/SDC drainlines, in instrument lines or during FMCRD replacement operations) would divert reactor vessel water into the lower drywell and, if these hatches were open, into the reactor building, potentially menacing safety equipment and rendering the core non-coolable.

It is therefore recommended that:

- the lower drywell hatches (equipment and personnel) remain open only when personnel are working inside the lower drywell, and never left open otherwise
- maintenance procedures requiring entry into the lower drywell should specify that in case of an RPV draining event, personnel must close these hatches before leaving the area

Prevention of Intersystem LOCA

The RWCU isolation valves for low flow configuration (reactor cleanup mode) must be capable of automatically isolating against a differential pressure equal to the operating pressure of the reactor coolant system in the event of a LOCA in the RWCU. If the automatic isolation valves fail to close, the operator can close the remote manual shutoff valve from the control room to terminate the LOCA.

The feedwater system containment isolation check valves provide an automatic capability to isolate the RPV coolant losses in case of feedwater pipe breaks outside of containment.

The main steam system has automatic isolation valves to close the RPV boundary and stop the coolant losses in case of pipe failure.

Important Structures, Systems and Components for Suppression Pool Bypass Analysis

Failure of a DW-WW vacuum breaker to close following an event requiring PCCS function would affect functionality of PCCS and in the long term would result in the need to open prematurely the containment bleed valves of CIS. If the containment bleed valves are open and one of the vacuum breakers has not closed there would be a direct pathway from the drywell to the wetwell vapor space to the environment.

The following are critical to assuring a low risk from wetwell/drywell vacuum breaker bypass:

- A low probability of vacuum breaker leakage
- A low probability that the vacuum breakers fail to close

19.6 REGULATORY TREATMENT OF NON-SAFETY SYSTEMS

19.6.1 Introduction and Background

The ESBWR plant design uses passive safety systems to supply safety injection water and provide core and containment cooling. The ESBWR design does not include any safety-related sources of AC power for the operation of passive system components. All active systems requiring AC power to operate are designated as nonsafety-related. Because the ESBWR relies on passive safety systems to perform the design-basis, safety-related functions of reactor inventory control and decay heat removal, different portions of the passive systems also provide certain defense-in-depth backup to the primary passive features. For example, while the Isolation Condenser System (ICS) is the primary safety-related heat removal and inventory control feature in a non-loss-of-coolant transient, the automatic depressurization system (ADS), together with the Gravity Driven Cooling System (GDCS), provides a safety-related, defense-in depth backup.

The ALWR Utility Requirements Document (URD) for passive plants, issued by the Electric Power Research Institute (EPRI), recommends that the plant designer specifically define the active systems relied upon for defense-in-depth. Defense-in-depth systems provide long-term, post-accident plant capabilities. Passive systems are able to perform their safety functions for 72 hours after an initiating event. After 72 hours, non-safety or active systems may be required to replenish the passive systems or to perform core and containment heat removal duties directly. The ESBWR includes active systems that provide defense-in-depth capabilities for reactor coolant system makeup and decay heat removal. These active systems are the first line of defense in reducing challenges to the passive systems in the event of transients or plant upsets. Most of these systems are designated as nonsafety-related.

For these defense-in-depth systems to operate, the associated systems and structures to support these functions must also be operable, such as nonsafety-related standby diesel generators.

In SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor Designs,” dated April 2, 1993, the staff discussed the issue of the regulatory treatment of non-safety systems (RTNSS) and stated that it would propose a process for resolution of this issue in a separate Commission paper. The staff subsequently issued SECY-94-084, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs,” dated March 28, 1994 (Reference 19.6-1), which discusses that process. SECY-95-132, “Policy and Technical Issues Associated with the Regulatory Treatment of Non-Safety Systems in Passive Plant Designs (SECY-94-084),” dated May 22, 1995, was essentially a revised version of SECY-94-084 issued to respond to Commission comments on that paper and to request Commission approval of certain revised positions. However, the staff’s position on RTNSS as discussed in SECY-94-084 was approved by the Commission (staff requirements memorandum (SRM) dated June 30, 1994), and was unchanged in SECY-95-132.

In SECY-94-084, the staff cited the uncertainties inherent in the use of passive safety systems resulting from limited operational experience and the relatively low driving forces (e.g., density differences and gravity) in these systems. The uncertainties relate to both system performance characteristics (e.g., the possibility that check valves could stick under low differential pressure conditions) and thermal-hydraulic phenomena (e.g., critical flow through ADS valves). The residual uncertainties associated with passive safety system performance increase the importance of active systems in providing defense-in-depth functions to back up the passive systems. Recognizing this, the NRC and EPRI developed a process to identify important active systems and to maintain appropriate regulatory oversight of those systems. This process does not require that the active systems brought under regulatory oversight meet all safety-related criteria, but rather that these controls provide a high level of confidence that active systems having a significant safety role are available when they are challenged.

19.6.2 Description of the RTNSS Process

Objectives

SECY-94-084 (Reference 19.6-1) identified a process for resolving the regulatory treatment of non-safety systems (RTNSS) issue. This process included the use of both probabilistic and deterministic criteria to achieve the following objectives:

- Determine whether regulatory oversight for certain non-safety-related systems was needed,
- Identify risk important SSCs for regulatory oversight (if it were determined that regulatory oversight was needed)
- Decide on an appropriate level of regulatory oversight for the various identified SSCs commensurate with their risk importance.

Probabilistic Criteria

The following PRA (including severe accident) related criteria are used to achieve the RTNSS process objectives:

- The ESBWR design should meet the Commission’s safety goal guideline for CDF of less than 1E-04/yr using a “focused PRA” which provides no credit for the performance of any non-safety-related "defense-in-depth" systems for which there will be no regulatory oversight according to the RTNSS process.
- The ESBWR design should meet the Commission's safety goal guideline for LRF of less than 1E-06/yr using a “focused PRA” which provides no credit for the performance of the non-safety-related "defense-in-depth" systems for which there will be no regulatory oversight according to the RTNSS process.
- SSC functions needed to meet the deterministic containment performance goal (SECY-93-087, Issue I.J), including containment bypass (SECY-93-087, Issue II.G), during severe accidents.

In applying the probabilistic criteria, the RTNSS process stresses the importance of accounting for uncertainties and also taking into consideration the risk importance of SSCs contributing to initiating event frequencies.

Specifically, the RTNSS process provides that the following two items must be addressed:

- Uncertainties, such as in the assumed reliability values for passive system components.

- Non-Safety-related SSCs contributing to initiating event frequencies could be subject to regulatory oversight, which is commensurate with their reliability/availability missions.

Deterministic Criteria

In addition to the probabilistic criteria, Reference 19.6-1, Attachment 2, Section A.I applies the following deterministic RTNSS criteria to meet the objectives:

- SSC functions relied upon to meet beyond design basis deterministic NRC performance requirements such as 10 CFR 50.62 for anticipated transient without scram (ATWS) mitigation and 10 CFR 50.63 for station blackout (SBO).
- SSC functions relied upon to resolve long-term safety (beyond 72 hours) and to address seismic events.
- SSC functions relied upon to prevent significant adverse systems interactions.

19.6.3 Review of ESBWR Against Deterministic RTNSS Criteria

Each of the deterministic RTNSS criteria above has been reviewed against the ESBWR design in DCD Chapter 1 Appendix D. The results are summarized in Table 1D-1 which provides a list of the systems and components that qualify for RTNSS consideration.

19.6.4 Review of ESBWR Against Probabilistic RTNSS Criteria

The ESBWR comprehensive baseline PRA described earlier in this chapter was used to evaluate plant performance against the probabilistic criteria identified above which are used to meet the RTNSS objectives. Consideration is also given to the uncertainty associated with the performance analysis of passive system components and to non-safety SSCs contributing to initiating event frequencies.

19.6.4.1 Focused PRA Analysis

A quantification of the ESBWR comprehensive baseline PRA was performed with the assumption of non-mechanistic failure of all non-safety related systems except for manual operation for the Fie Protection System to refill the PCCS/ICS pools at the end of 24 hours. This action provides continuous containment heat removal in the case where the inter-pool connection valves fail. The results indicate that the core damage frequency safety goal of 10-4/yr is met.

The LRF goal of 10-6/yr is also met using the same assumptions.

The portions of the FPS that provide makeup to the pools are also identified in the deterministic analysis in Chapter 1, Appendix D. In this case, it is identified as required to provide continued containment heat removal beyond 72 hours based upon the deterministic criterion. The PRA analysis only includes operation of the FPS in a mode that is independent of any other system interfaces such as FAPCS, that are not credited in the analysis.

19.6.4.2 Passive System Performance Uncertainty

The performance uncertainty of the passive systems is accounted for in the ESBWR design by increased design redundancies in the key passive systems and components. This is discussed below for each of the passive safety systems.

Passive Containment Cooling System (PCCS)

The PCCS includes 6 passive heat exchangers. The system is fully passive in that there are no active components that are required in order for the system to perform its design function. In addition, the success criterion for this system is that only 4 of the 6 heat exchangers must function. This provides a significant uncertainty allowance.

Gravity Driven Cooling System (GDCS)

There is significant design allowance in this system as follows

- Only 2 out of 3 GDCS Pools are required
- Only 2 out of 8 lines connecting the GDCS to the RPV are required
- Only 1 out of 4 equalizing lines is required

Automatic Depressurization System (ADS)

This system has 8 depressurization valves (DPVs). Only 4 are required to reduce RPV pressure to allow for GDCS flow into the RPV. Each of the 8 lines also includes biased-open swing check valves.

Isolation Condenser System (ICS)

Three (3) out of 4 ICs are required. The uncertainty associated with this system is considerably less than other passive systems because of the significant operating experience with ICs in the current generation of plants. An ICS was included in the first BWRs built and the performance information on these systems is extensive.

19.6.5 Results

As a result of the focused PRA analysis, it was concluded that the core damage frequency and the LRF criteria are met if credit is provided to the use of the non-safety Fire Protection System for IC/PCC pool make-up.

The portions of the FPS that are required to perform this pool make-up function can be considered for RTNSS designation.